

<http://v3.espacenet.com/publicationDetails/biblio?DB=EPODOC&adjacent=true&|...> 2010/01/28

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-78519

(P2003-78519A)

(43) 公開日 平成15年3月14日 (2003.3.14)

(51) Int.Cl. ⁷	識別記号	F I	データ* (参考)
H 0 4 L 9/14		G 0 6 F 17/60	1 4 2 5 J 1 0 4
G 0 6 F 17/60	1 4 2		3 0 2 E
	3 0 2		5 1 2
	5 1 2	G 0 9 C 5/00	
G 0 9 C 5/00		H 0 4 L 9/00	6 4 1
審査請求 未請求 請求項の数35 O L (全 28 頁)			

(21) 出願番号 特願2002-161440(P2002-161440)

(22) 出願日 平成14年6月3日 (2002.6.3)

(31) 優先権主張番号 特願2001-168259(P2001-168259)

(32) 優先日 平成13年6月4日 (2001.6.4)

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願2001-172451(P2001-172451)

(32) 優先日 平成13年6月7日 (2001.6.7)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 シェン メイ・シェン

シンガポール534415シンガポール、タイ・

セン・アベニュー、ブロック1022、04-

3530番、タイ・セン・インダストリアル・

エステイト、パナソニック・シンガポール

研究所株式会社内

(74) 代理人 100062144

弁理士 青山 榛 (外1名)

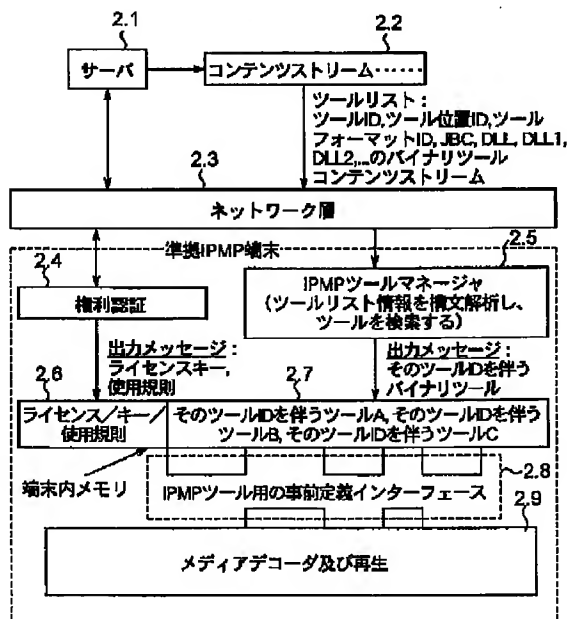
最終頁に続く

(54) 【発明の名称】 コンテンツ提供及び保護用の柔軟及び共通 IPMP システムの装置及び方法

(57) 【要約】

【課題】 柔軟及び共通 IPMP システム (知的所有権管理及び保護) の装置は、コンテンツストリームに保持された、又は URL 位置からダウンロードされた完全な IPMP ツールリストを取り入れることにより柔軟性及び相互運用性を与える。

【解決手段】 前処理モジュールとして機能する準拠 IPMP 端末の IPMP ツールマネージャを提供して、IPMP ツールリストを構文解析し、IPMP ツール ID、それに関連する位置識別子及び IPMP ツールフォーマット ID に基づいて IPMP ツールを取得する。IPMP ツールを、バイナリフォーマットにプリコンパイルして IPMP 端末に伝送又はダウンロードすることができ、IPMP 端末の異なるプラットフォーム上の対象に対して異なるバイナリフォーマットをコンテンツプロバイダにより用意する。



【特許請求の範囲】

【請求項 1】 符号化技術を用いてコンテンツをコンテンツストリームに符号化する手段と、
データ暗号化ツールを用いて当該符号化コンテンツストリームを暗号化する手段と、
透かしツールを用いて当該コンテンツに透かし情報を埋め込む手段と、

上記ステップで用いられた当該コンテンツに関するコンテンツ ID 及び I PMP（知的所有権管理保護）ツールリスト（I PMP ツール情報）を作成する手段と、
各コンテンツストリームのヘッダとして保持すべき I PMP ツールリストフラグを作成する手段と、
I PMP ツールリストフラグ、次いで I PMP ツールリスト、コンテンツ ID 及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成する手段と、
を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟 I PMP システムの装置。

【請求項 2】 符号化技術を用いてコンテンツをコンテンツストリームに符号化する手段と、
データ暗号化ツール又は他のツールを用いた当該符号化コンテンツストリームを暗号化する手段と、

上記ステップで用いられた当該コンテンツに関するコンテンツ ID 及び I PMP（知的所有権管理保護）ツールリスト（I PMP ツール情報）を作成する手段と、
各コンテンツストリームのヘッダとして保持すべき I PMP ツールリストフラグを作成する手段と、
I PMP ツールリストフラグ、次いで I PMP ツールリスト、コンテンツ ID 及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成する手段と、
を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟 I PMP システムの装置。

【請求項 3】 符号化技術を用いてコンテンツをコンテンツストリームに符号化する手段と、
暗号化キーを有する暗号化ツール又は他のツールを用いて当該コンテンツストリームを暗号化する手段と、
より高いセキュリティのために別の暗号化キーを有する任意の暗号化ツールを用いて当該暗号化キーを暗号化する手段と、

当該コンテンツストリームと同一のストリームに保持された I PMP 情報に上記当該暗号化されたキーを埋め込む手段と、

上記ステップで使われた当該コンテンツに関するコンテンツ ID 及び I PMP（知的所有権管理保護）ツールリスト（I PMP ツール情報）を作成する手段と、
各コンテンツストリームのヘッダとして保持すべき I PMP ツールリストフラグを作成する手段と、

I PMP ツールリストフラグ、次いで I PMP ツールリスト、コンテンツ ID 及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成する手段と、
を含む、コンテンツプロバイダ側のコンテンツ提供及び

保護用の柔軟 I PMP システムの装置。

【請求項 4】 請求項 1、2 及び 3 において当該コンテンツに関するコンテンツ ID 及び I PMP ツールリストを作成することが、

I PMP ツール ID を各コンテンツに割当てて、何れのツールをデータ保護に使用するかを表示する手段と、
位置タイプ ID を各 I PMP ツールに割当てて、当該 I PMP ツールが入手可能である位置のタイプを通知する手段と、

10 フォーマット ID を割当てて、ダウンロードされた I PMP ツールフォーマットを表示して、準拠 I PMP 端末がそれらのプラットフォームに基づいて選択及び検索することを可能にする手段と、

当該 I PMP ツールの位置を表示して、端末が当該 I PMP ツールを当該位置から取得することを可能にする手段と、

を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟 I PMP システムの装置。

【請求項 5】 I PMP 端末の I PMP ツールマネージャでコンテンツストリームの中を構文解析する手段と、
I PMP ツールリストフラグ、コンテンツ ID 及び I PMP ツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I PMP ツールリストに基づいて I PMP ツールを取得する手段と、
を含む、I PMP 端末側のコンテンツ提供及び保護用の柔軟 I PMP システムの装置。

【請求項 6】 I PMP 端末の I PMP ツールマネージャでコンテンツストリームの中を構文解析する手段と、
I PMP ツールリストフラグ、コンテンツ ID 及び I PMP ツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I PMP ツールリストに基づいて I PMP ツールを取得する手段と、

要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行う手段と、

前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信する手段と、

前記ユーザ権利認証が成功した後、要求されたコンテンツの消費用の使用規則を取得する手段と、

を含む、I PMP 端末側のコンテンツ提供及び保護用の柔軟 I PMP システムの装置。

【請求項 7】 要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行う手段と、
前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信する手段と、

当該ライセンス又はキー情報を I PMP 端末で構文解析

する手段と、
当該ライセンス又はキー情報を当該I PMP端末のメモリに格納する手段と、

当該I PMP端末のI PMPツールマネージャでコンテンツストリームの中を構文解析する手段と、

I PMPツールリストフラグ、コンテンツID及びI PMPツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該I PMPツールリストに基づいてI PMPツールを取得する手段と、

I PMPツールリスト情報の当該部分と共に上記ステップで検索された当該I PMPツールを当該I PMP端末のメモリに格納する手段と、

当該メモリに格納された当該I PMPツールと共に当該ライセンス／キー情報を用いて当該コンテンツストリームを暗号解読及び復号する手段と、

を含む、I PMP端末側のコンテンツ提供及び保護用の柔軟及び共通I PMPシステムの装置。

【請求項8】 要求をコンテンツディストリビュータに送信して、ユーザ認証を行う手段と、

当該コンテンツディストリビュータからライセンス又はキー情報を受信する手段と、

当該ライセンス又はキー情報をI PMP端末で構文解析する手段と、

当該ライセンス又はキー情報を当該I PMP端末のメモリに格納する手段と、

当該I PMP端末のI PMPツールマネージャでコンテンツストリームの中を構文解析する手段と、

I PMPツールリストフラグ、コンテンツID及びI PMPツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該I PMPツールリストに基づいてI PMPツールを取得する手段と、

I PMPツールリスト情報の当該部分と共に上記ステップで検索された当該I PMPツールを当該I PMP端末のメモリに格納する手段と、

当該ライセンス又はキー情報を用いて当該I PMP情報内の当該暗号化されたキーを暗号解読する手段と、

コンテンツプロバイダ側で当該コンテンツを暗号化するために使用された暗号化キーを上記ステップから取得する手段と、

上記ステップから取得された当該暗号化キーを用いて当該コンテンツを暗号解読して、最初のコンテンツを取得する手段と、

当該最初のコンテンツを当該I PMP端末での再生のために復号する手段と、を含む、I PMP端末側のコンテンツ提供及び保護用の柔軟及び共通I PMPシステムの装置。

【請求項9】 請求項5、6、7、8のいずれかにおいてI PMPツールリストは、

I PMPツールの大部分に関するI PMPツールIDをテーブル状に定義しており、

当該テーブルに予約可能な未使用スペースがあり、

I PMPツールタイプとも呼ばれるI PMPツールのカテゴリとしてI PMPツールIDの一部が定義されており、

当該テーブルをI PMP端末に事前ロード、事前符号化又はダウンロードする手段と、

前記コンテンツストリーム内に保持された当該I PMPツールリストから当該I PMPツールIDを抽出する手段と、

前記コンテンツストリームに保持された当該I PMPツールリストに表示されたI PMPツール位置識別子を取得する手段と、

I PMPツール位置識別子に加えて、I PMPツールIDと共に、当該コンテンツストリームに保持されたI PMPツールフォーマットIDを取得する手段と、

適切なフォーマットであるI PMPツールを選択して、

I PMP端末プラットフォームに適合させる手段と、

上記手段で取得された当該位置から当該I PMPツールを検索する手段と、とを更に含む、I PMP端末側のコンテンツ提供及び保護用の柔軟及び共通I PMPシステムの装置。

【請求項10】 予め定めたテーブルに基づいてI PMPツールリストを構築してコンテンツに使用されたI PMPツールの内容をI PMP端末に通知することが、

データ暗号解読、透かしなどのI PMPツールのカテゴリとして当該予め定めたテーブルからI PMPツールタイプIDを選択する手段と、

当該I PMPツールタイプIDの下である特定のアルゴリズムを有するある特定のI PMPツールに関して当該予め定めたテーブルからI PMPツールIDを選択する手段と、

当該予め定めたテーブルからI PMPツール位置IDを選択して、I PMPツールをダウンロード又は検索可能な場所を通知する手段と、

I PMPツールを遠隔で検索する場合、当該I PMPツールリストにURL位置を与える手段と、

バイナリフォーマットにプリコンパイルされたI PMPツールの各セットに関するI PMPツールフォーマットIDを選択する手段と、を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通I PMPシステムの装置。

【請求項11】 請求項1、2、3のいずれかにおいて暗号化ツールを用いて事前符号化コンテンツストリームを暗号化することが、

イントラ符号化フレーム（I フレーム）などの事前符号化映像ストリームでキーアクセスユニットを探索する手

段と、
 すべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該キーアクセスユニットのみを暗号化して、暗号解読側の処理を高速化する手段と、を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通I PMPシステムの装置。

【請求項12】 請求項1、2、3のいずれかにおいて暗号化ツールを用いて事前符号化コンテンツストリームを暗号化することが、

事前符号化映像ストリーム又は音声ストリームで重要ビットを探索する手段と、

すべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該重要ビットのみを暗号化して、暗号解読側の処理を高速化する手段と、を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通I PMPシステムの装置。

【請求項13】 請求項11または12において選択されたアクセスユニット又は重要ビットに関して暗号化を部分的に行われた保護コンテンツストリームを復号する手段と、

予め定めた規則に基づいて暗号化されたビット又はアクセスユニットを探索して、所与のデータ暗号解読ツールを用いて前記ビット又はアクセスユニットを暗号解読する手段と、を含む、保護コンテンツを暗号解読して再生するI PMP端末側のコンテンツ提供及び保護用の柔軟及び共通I PMPシステムの装置。

【請求項14】 指定インタフェースに従ってI PMPツールがされており、

当該インタフェースを含んだI PMP端末が構築されたI PMPシステムの装置において、

当該I PMPツールを検索して当該端末の当該インタフェースに適合させる手段を含む、コンテンツ提供及び保護用の柔軟及び共通I PMPシステムの装置。

【請求項15】 MPEG-4システムにある基本ストリームに対応付けられたデコーダ構成記述子に新しいストリームタイプを指定し、

MPEG-4のI PMP基本ストリームにI PMPツールを保持することを可能にした、コンテンツ提供及び保護用の柔軟及び共通I PMPシステムの装置。

【請求項16】 符号化技術を用いてコンテンツをコンテンツストリームに符号化するステップと、

データ暗号化ツールを用いて当該符号化コンテンツストリームを暗号化するステップと、

透かしツールを用いて当該コンテンツに透かし情報を埋め込むステップと、

上記ステップで用いられた当該コンテンツに関するコンテンツID及びI PMP（知的所有権管理保護）ツールリスト（I PMPツール情報）を作成するステップと、各コンテンツストリームのヘッダとして保持すべきI PMPツールリストフラグを作成するステップと、

I PMPツールリストフラグ、次いでI PMPツールリスト、コンテンツID及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成するステップと、を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通I PMPシステムの方法。

【請求項17】 符号化技術を用いてコンテンツをコンテンツストリームに符号化するステップと、

データ暗号化ツール又は他のツールを用いて当該符号化コンテンツストリームを暗号化するステップと、

上記ステップで用いた当該コンテンツに関するコンテンツID及びI PMP（知的所有権管理保護）ツールリスト（I PMPツール情報）を作成するステップと、

各コンテンツストリームのヘッダとして保持すべきI PMPツールリストフラグを作成するステップと、

I PMPツールリストフラグ、次いでI PMPツールリスト、コンテンツID及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成するステップと、を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通I PMPシステムの方法。

【請求項18】 符号化技術を用いてコンテンツをコンテンツストリームに符号化するステップと、

暗号化キーを有する暗号化ツール又は他のツールを用いて当該コンテンツストリームを暗号化するステップと、より高いセキュリティのために別の暗号化キーを有する任意の暗号化ツールを用いて当該暗号化キーを暗号化するステップと、

当該コンテンツストリームと同一のストリームに保持されたI PMP情報に上記当該暗号化されたキーを埋め込むステップと、

上記ステップで用いた当該コンテンツに関するコンテンツID及びI PMP（知的所有権管理保護）ツールリスト（I PMPツール情報）を作成するステップと、各コンテンツストリームのヘッダとして保持すべきI PMPツールリストフラグを作成するステップと、

I PMPツールリストフラグ、次いでI PMPツールリスト、コンテンツID及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成するステップと、を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟I PMPシステムの方法。

【請求項19】 請求項16、17、18のいずれかにおいて当該コンテンツに関するコンテンツID及びI PMPツールリストを作成することが、

I PMPツールIDを各コンテンツに割当てて、何れのツールをデータ保護に使用するかを表示するステップと、

位置タイプIDを各I PMPツールに割当てて、当該I PMPツールが入手可能である位置のタイプを通知するステップと、

フォーマットIDを割当てて、ダウンロードされたI PMPツールフォーマットを表示して、準拠I PMP端末

がそれらのプラットフォームに基づいて選択及び検索することを可能にするステップと、

当該 I PMP ツールの位置を表示して、端末が当該 I PMP ツールを当該位置から取得することを可能にするステップと、を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟 I PMP システムの方法。

【請求項 20】 I PMP 端末の I PMP ツールマネージャでコンテンツストリームの中を構文解析するステップと、

I PMP ツールリストフラグ、コンテンツ ID 及び I PMP ツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I PMP ツールリストに基づいて I PMP ツールを取得するステップと、

を含む、I PMP 端末側のコンテンツ提供及び保護用の柔軟 I PMP システムの方法。

【請求項 21】 I PMP 端末の I PMP ツールマネージャでコンテンツストリームの中を構文解析するステップと、

I PMP ツールリストフラグ、コンテンツ ID 及び I PMP ツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I PMP ツールリストに基づいて I PMP ツールを取得するステップと、

要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行うステップと、

前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信するステップと、

前記ユーザ権利認証が成功した後、要求されたコンテンツの消費の使用規則を取得するステップと、

を含む、I PMP 端末側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの方法。

【請求項 22】 要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行うステップと、前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信するステップと、

当該ライセンス又はキー情報を I PMP 端末で構文解析するステップと、

当該ライセンス又はキー情報を当該 I PMP 端末のメモリに格納するステップと、

当該 I PMP 端末の I PMP ツールマネージャでコンテンツストリームの中を構文解析するステップと、

I PMP ツールリストフラグ、コンテンツ ID 及び I PMP ツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I PMP

ツールリストに基づいて I PMP ツールを取得するステップと、

I PMP ツールリスト情報の当該部分と共に上記ステップで検索された当該 I PMP ツールを当該 I PMP 端末のメモリに格納するステップと、

当該メモリに格納された当該 I PMP ツールと共に当該ライセンス／キー情報を用いて当該コンテンツストリームを暗号解読及び復号するステップと、を含む、I PMP 端末側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの方法。

【請求項 23】 要求をコンテンツディストリビュータに送信して、ユーザ認証を行うステップと、

当該コンテンツディストリビュータからライセンス又はキー情報を受信するステップと、

当該ライセンス又はキー情報を I PMP 端末で構文解析するステップと、

当該ライセンス又はキー情報を当該 I PMP 端末のメモリに格納するステップと、

当該 I PMP 端末の I PMP ツールマネージャでコンテンツストリームの中を構文解析するステップと、

I PMP ツールリストフラグ、コンテンツ ID 及び I PMP ツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I PMP ツールリストに基づいて I PMP ツールを取得するステップと、

I PMP ツールリスト情報の当該部分と共に上記ステップで検索された当該 I PMP ツールを当該 I PMP 端末のメモリに格納するステップと、

当該ライセンス又はキー情報を用いて当該 I PMP 情報内の当該暗号化されたキーを暗号解読するステップと、コンテンツプロバイダ側で当該コンテンツを上記ステップで暗号化するために使用された暗号化キーを取得するステップと、

上記ステップから取得された当該暗号化キーを用いて当該コンテンツを暗号解読して、最初のコンテンツを取得するステップと、

当該最初のコンテンツを当該 I PMP 端末で再生する為に復号するステップと、を含む、I PMP 端末側のコンテンツ提供及び保護用の柔軟及び共通 I PMP システムの方法。

【請求項 24】 請求項 20、21、22、23 のいずれかにおいてローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該 I PMP ツールリストに基づいて I PMP ツールを取得することが、

I PMP ツールの大部分に関する I PMP ツール ID をテーブルに定義されており、

今後の又は未知／専用の I PMP ツールに使用されるべき I PMP ツール ID に関する項目を当該テーブルに予

50

約する余地があり、
I PMP ツールタイプとも呼ばれる I PMP ツールのカ
テゴリとして I PMP ツール ID の一部が定義されてい
る、
当該テーブルを I PMP 端末に事前ロード、事前符号化
又はダウンロードするステップと、
前記コンテンツストリーム内に保持された当該 I PMP
ツールリストから当該 I PMP ツール ID を抽出するス
テップと、
前記コンテンツストリームに保持された当該 I PMP ツ
ールリストに表示された I PMP ツール位置識別子を取
得するステップと、
I PMP ツール位置識別子に加えて、I PMP ツール ID
と共に、当該コンテンツストリームに保持された I P
MP ツールフォーマット ID を取得するステップと、
適切なフォーマットである I PMP ツールを選択して、
I PMP 端末プラットフォームに適合させるステップ
と、
上記手段で取得された当該位置から当該 I PMP ツール
を検索するステップと、を更に含む、I PMP 端末側の
コンテンツ提供及び保護用の柔軟及び共通 I PMP シス
テムの方法。

【請求項 25】 予め定めたテーブルに基づいて I PM
P ツールリストを構築して、コンテンツに使用された I
PMP ツールの内容を I PMP 端末に通知するステップ
と、
対応するコンテンツストリームの前に当該 I PMP ツ
ールリストを挿入するステップと、を含む、コンテンツプ
ロバイダ側のコンテンツ提供及び保護用の柔軟及び共通
I PMP システムの方法。

【請求項 26】 予め定めたテーブルに基づいて I PM
P ツールリストを構築してコンテンツに使用された I P
MP ツールの内容を I PMP 端末に通知することが、
データ暗号解読、透かしなどの I PMP ツールのカテゴ
リとして当該予め定めたテーブルから I PMP ツールタ
イプ ID を選択するステップと、
当該 I PMP ツールタイプ ID の下である特定のアルゴ
リズムを有するある特定の I PMP ツールに関して当該
予め定めたテーブルから I PMP ツール ID を選択する
ステップと、
当該予め定めたテーブルから I PMP ツール位置 ID を
選択して、I PMP ツールをダウンロード又は検索可能
な場所を通知するステップと、
I PMP ツールを遠隔で検索する場合、当該 I PMP ツ
ールリストに URL 位置を与えるステップと、
バイナリフォーマットにプリコンパイルされた I PMP
ツールの各セットに関する I PMP ツールフォーマット
ID を選択するステップと、
を更に含む、コンテンツプロバイダ側のコンテンツ提供
及び保護用の柔軟及び共通 I PMP システムの方法。

【請求項 27】 請求項 16、17、18 のいずれかに
おいて暗号化ツールを用いて事前符号化コンテンツス
トリームを暗号化することが、
イントラ符号化フレーム（I フレーム）などの事前符号
化映像ストリームでキーアクセスユニットを探索するス
テップと、
すべてのアクセスユニットを暗号化する代わりに暗号化
ツールを用いて当該キーアクセスユニットのみを暗号化
して、暗号解読側の処理を高速化するステップと、を更
に含む、コンテンツプロバイダ側のコンテンツ提供及び
保護用の柔軟及び共通 I PMP システムの方法。

【請求項 28】 請求項 16、17、18 のいずれかに
おいて暗号化ツールを用いて事前符号化コンテンツス
トリームを暗号化することが、
事前符号化映像ストリーム又は音声ストリームで重要ビ
ットを探索するステップと、
すべてのアクセスユニットを暗号化する代わりに暗号化
ツールを用いて当該重要ビットのみを暗号化して、暗号
解読側の処理を高速化するステップと、を更に含む、コ
ンテンツプロバイダ側のコンテンツ提供及び保護用の柔
軟及び共通 I PMP システムの方法。

【請求項 29】 請求項 27 または 28 において選択さ
れたアクセスユニット又は重要ビットに関して暗号化を
部分的に行うことが、
保護コンテンツストリームを復号するステップと、
予め定めた規則に基づいて暗号化されたビット又はアク
セスユニットを探索して、所与のデータ暗号解読ツール
を用いて前記ビット又はアクセスユニットを暗号解読す
るステップと、を含む、保護コンテンツを暗号解読して
再生する I PMP 端末側のコンテンツ提供及び保護用の
柔軟及び共通 I PMP システムの方法。

【請求項 30】 MPEG-4 システムにある基本スト
リームに対応付けられたデコーダ構成記述子に新しいス
トリームタイプを指定して、
MPEG-4 の I PMP 基本ストリームに I PMP ツ
ールを保持することを可能にした、コンテンツ提供及び保
護用の柔軟及び共通 I PMP システムの方法。

【請求項 31】 暗号化されたコンテンツと、その解読鍵
と、解読モジュールと、コンテンツの利用規則と、利用
規則管理モジュールを持つプロバイダと、ネットワーク
を通じて接続されたユーザ端末から構成され、プロバイ
ダ側で、ユーザ端末に送るメッセージ中に、更新すべき
ソフトウェアモジュールの識別子とその存在する場所を
示す情報を含めることにより、ユーザ端末に著作権保護
システムの更新を行わせ、更新すべきソフトウェアモジ
ュールは、解読モジュールと利用規則管理モジュールを
含むことにより、プロバイダの意図する利用規則に従っ
てコンテンツの解読・視聴を行うことを特徴とするコン
テンツ提供及び保護用の柔軟及び変通 I PMP システム
の装置。

【請求項 3 2】暗号化されたコンテンツと、その解読鍵と、解読モジュールと、コンテンツの利用規則と、利用規則管理モジュールを持つプロバイダと、ネットワークを通じて接続されたユーザ端末から構成され、ユーザ端末は、プロバイダから利用規則管理モジュールを受け取って自身に組み込み、これを用いて、プロバイダから受け取る著作権保護情報の中にある、コンテンツの利用規則に従い、プロバイダから受け取るコンテンツの再生を行うことを特徴とするコンテンツ提供及び保護用の柔軟及び変通 I PMP システムの装置。

【請求項 3 3】利用規則は、コンテンツの利用可能期間、無料再生可能時間、再生可能回数、コピー可能回数、移動可能回数のいずれかを含むことを特徴とする請求項 3 1 または 3 2 に記載のコンテンツ提供及び保護用の柔軟及び変通 I PMP システムの装置。

【請求項 3 4】プロバイダからユーザ端末に送られるメッセージは、メッセージ項目名と直後に続くメッセージ項目の値の組で構成され、ユーザ端末に送るメッセージ項目の順序を問わないことを特徴とする、請求項 3 1 または 3 2 に記載のコンテンツ提供及び保護用の柔軟及び変通 I PMP システムの装置。

【請求項 3 5】ユーザ端末からプロバイダに送られるメッセージは、ユーザ端末情報を含むことにより、ユーザ端末に適合するモジュールをプロバイダから受信することが出来ることを特徴とする請求項 3 1 または 3 2 に記載のコンテンツ提供及び保護用の柔軟及び変通 I PMP システムの装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンテンツの提供及び保護に関し、特に保護コンテンツを異なる I PMP システムにより消費する、及び同一コンテンツを異なる I PMP システムにより保護するような用途に関する。

【0002】

【従来の技術】コンテンツ提供は、マルチメディアデータとして益々需要が増大しており、コンテンツは、どこへでもいつでも到達可能である。ユーザは、便利さ及び柔軟性に満足しており、娯楽を容易かつ効率的に楽しむことができる。

【0003】一方、コンテンツの所有者は、顧客のニーズを満たすように努力しているが、同時に、それらのプロパティの不正使用にも苦慮している。2つの側面の間のバランスである。

【0004】前記コンテンツを保護する保護技法は、データ暗号化、透かし、暗号手法など多数ある。前記保護技法は、多くのコンテンツ提供アプリケーションで実施されている。異なるシステムが異種の機構及び保護技法を使用して保護付きのコンテンツを提供するように見える。その場合におけるすべての端末又はコンテンツ消費装置は、同一のコンテンツプロバイダにより提供される

コンテンツを実行して消費することができるだけである。前記保護技法では、それらの端末又は装置を交換して異なるコンテンツを再生することはできない。

【0005】MPEG 標準化グループにおいて、人々は、準拠端末を含む I PMP システムを標準化する方へ努力している。すべての端末は、たとえどのような種類の I PMP ツールを使用しても、次のような同一の I PMP 標準により暗号化されて保護される保護コンテンツを再生することができる。

10 【0006】そのような端末は音声及び映像デコーダのようなコンテンツデコーダから成り、更に、前記端末は、前記コンテンツを復号して再生できる前に前記保護コンテンツから保護を解除する必要がある。従って、I PMP ツールリストを含む保護情報は、保護を解除する方法を理解するのに必要とされ、前記端末がコンテンツを利用するのに必要とされる。

20 【0007】一方、I PMP ツールは予めある特定のツールに固定されない。これは、ベンダがそれらの I PMP システムで好みのツールを選択する柔軟性をより高めることである。このような場合、より高い柔軟性とセキュリティの両方を同時に提供するのにある標準の方法及びインタフェースを定義する必要がある。

【0008】そのような端末に関する先行技術が基本的に図 1 に示してあり、図 1 は、リアルタイムでユーザ認証、I PMP ツール検索及びコンテンツ復号までの作業の流れを示す。

【0009】異なるベンダは、同一のコンテンツデコーダ、例えば MPEG-2 又は MPEG-4 を使用するけれども、前記先行技術におけるユーザ認証及び I PMP ツール検索は、異なるベンダに関して全く違って実施されている。このような場合に異なるコンテンツプロバイダにより提供される異なるコンテンツを実行するのに同一の端末を製造することは非常に困難である。換言すれば、同一の保護コンテンツを異なる I PMP システムで再生することができない。

【0010】

【発明が解決しようとする課題】解決すべき課題は、同一の I PMP システム構造を定義して異なる I PMP システムが同一の保護コンテンツを消費可能にすること、及び I PMP システム実施者に対して標準の方法を提供して安全な方法でエンコーダ、チャネル提供から端末までの全システムを構築することである。

【0011】

【課題を解決するための手段】本発明によれば、柔軟及び共通 I PMP システム（知的所有権管理及び保護）の装置は、コンテンツストリームに保持された、又は URL 位置からダウンロードされた完全な I PMP ツールリストを取り入れることにより柔軟性及び相互運用性を与える。

50 【0012】前処理モジュールとして機能する準拠 I P

MP端末のIPMPツールマネージャによって、IPMPツールリストを構文解析し、IPMPツールID、それに関連する位置識別子及びIPMPツールフォーマットIDに基づいてIPMPツールを取得する。

【0013】IPMPツールを、バイナリフォーマットにプリコンパイルしてIPMP端末に伝送又はダウンロードすることができるように、IPMP端末の異なるプラットフォーム上の対象に対して異なるバイナリフォーマットをコンテンツプロバイダにより用意する。

【0014】3種類の主要かつ一般的なインタフェースは、非常に有用かつ典型的な用途要件に従って、データ暗号解読、透かし埋め込み、及び透かし及びデータ暗号解読の仕方用に指定される。

【0015】本発明の一実施例では最小2層構造を提案して、ユーザ認証出力メッセージを指定し、異なるIPMPシステムに関してより高いセキュリティ及び端末互換性を与える。

【0016】端末複雑性及びIPMPツール多様性は、IPMPツールを取得して使用する際に異なるプロファイルを指定することにより処理される。

【0017】まず第1に、IPMPツールリストを、コンテンツストリーム内に位置するある特定のバケットとして定義し、下記の内容を示す。

- ・コンテンツを保護するのに使用されるIPMPツールのリスト

- ・ダウンロードされたIPMPツールのフォーマットID

- ・IPMPツールの位置タイプ

- ・IPMPツールを取得可能な位置

【0018】IPMPツールリストフラグは、上記バケットの前にヘッダとして位置している。

【0019】IPMPツールマネージャは、コンテンツデコーダの前に位置するあるモジュールとして設計され、コンテンツストリームに保持された、又はどこかに格納されたIPMPツールリストを構文解析して、コンテンツストリームから保護を取り外す為のIPMPツールを取得する。

【0020】汎用のインタフェースが、ダウンロードされたIPMPツールをIPMP端末で使用する様にIPMP端末用指定される。このインタフェースはある種のツールに基づいた殆どの異なるアルゴリズムを扱えるように定義される。

【0021】2層のセキュリティ構造を取り入れて、より高いセキュリティを与えると同時に、端末互換性のために任意の異なるユーザ認証方法に関する出力要件を決定する。

【0022】IPMPツールIDは予め定めたテーブルで定義され、前記テーブルを事前符号化又は端末にダウンロードしておいても良い。コンテンツプロバイダ側と端末側の両方は、同一のテーブルを参照して同一のIP

MPツールに同一のIPMPツールIDを使用する必要がある。

【0023】端末は、標準のIPMPツールと考えられているIPMPツールを事前に実装していても良いし、前記端末がダウンロード機能を有する場合、コンテンツストリームに保持されたIPMPツールリストに基づいて独自のIPMPツールをダウンロードしても良い。

【0024】暗号化キーは、前記2層セキュリティ構造に基づいて更に暗号化してIPMP情報に挿入され、コンテンツストリームと共に端末へ伝送される。

【0025】コンテンツプロバイダ側では、メディアコンテンツは、MPEG-2又はMPEG-4のような符号化技術を用いて符号化され、DES又はAESのようなIPMPツールを用いて暗号化される。前記コンテンツは、符号化前に透かしを埋め込まれても良い。

【0026】同時に、コンテンツIDは、コンテンツ著作権情報、コンテンツ作成情報などに基づいて生成される。また、IPMPツールリストは、コンテンツを保護する際に使用されるIPMPツールに基づいて生成される。前記IPMPツールリストは、IPMPツールID、IPMPツールフォーマットID、位置タイプ、IPMPツールの位置及び予約フィールドを含む。位置識別子は、位置タイプ及び位置詳細が特定のIPMPツールIDに従うので、特定のIPMPツールと密接に関連がある。

【0027】IPMPツールリストフラグは、その後続くものがIPMPツールリストであることを示す。

【0028】任意の端末は、そのようなコンテンツを取得又は検索できるが、適切な使用ライセンス及び対応する又は正しいIPMPツールなしに再生はできない。

【0029】端末側では、IPMPツールリストをIPMPツールマネージャモジュールに渡し、IPMPツールを取得する。

【0030】取得されたIPMPツールは、端末で使用可能なものであり、IPMP端末に格納されて予め定めたインタフェース用に用意がされる。

【0031】コンテンツストリームが、コンテンツデコーダを通過し始めると、IPMPシステムは、ユーザ認証モジュールを起動して、ユーザ端末ID、コンテンツID及びその他の関連情報を与えることによりコンテンツプロバイダ又は提供エージェントにセンス要求を送信する。ライセンスは、ユーザ認証がうまく行われた後、端末に発行される。

【0032】最後に、暗号化されたキーは暗号解読され、暗号化されたコンテンツも暗号解読され、コンテンツは端末で復号及び再生可能となる。

【0033】

【発明の実施の形態】図1は、現在の典型的なIPMP（知的所有権管理保護）システムを示す。

【0034】ユニット1. 0のコンテンツ所有者は、ユ

ニット1. 1、1. 5及び1. 9の異なるコンテンツプロバイダA、B及びCを通してコンテンツを提供する。異なるIPMPシステムは、3組のIPMPシステムで実施されている。

【0035】各々のプロトコルが異なるIPMPツール（例えば暗号化ツール）及び異なるユーザ認証ツールなどを使用しているので、IPMPツールを取得して検査する方法はそれら自体のプロトコルに基づく。異なるユーザ認証方法は、ユニット1. 2、1. 6及び1. 10に示してあり、IPMPツールを取得する異なる方法は、ユニット1. 3、1. 7及び1. 11に示してある。

【0036】従って、ユニット1. 4、1. 8及び1. 12に示すように、コンテンツ復号又はコンテンツ消費端末も互いに異なる。端末AがコンテンツプロバイダBにより提供される保護コンテンツを再生することはできないということが明らかである。

【0037】以下の内容については、本願発明者による先の出願（特願2001-058236）において解決された。

1) IPMPツール情報をストリームに保持して、コンテンツプロバイダ及びコンテンツディストリビュータにより何れのIPMPツールを使用するかを表示すること。

2) 準拠IPMP端末でIPMPツール管理を用いてIPMP情報を処理すること。

3) 異なる処理能力を有するIPMP端末に関するプロファイルを定義して、IPMPシステムを実現すること。

【0038】しかし、先の出願では未解決の問題点が2つあり、次のとおりである。

1) 端末OS及びプラットフォームに依存するダウンロードツールフォーマットの問題。

2) IPMP端末で使用されるべきIPMPツール用のインタフェースの問題。

【0039】本願では、更に、先の出願で提示されたIPMPシステムをより詳細かつより完全な形態で説明し、2つの問題点を詳細に扱って説明する。

【0040】図2は、MPEG-nのIPMPシステムを示す。

【0041】サーバは、モジュール2. 1で示され、コンテンツプロバイダかコンテンツディストリビュータの何れかとして機能し、又は異なる用途シナリオの場合には両方の機能を果たす。

【0042】ネットワーク層は、モジュール2. 3で示され、準拠IPMP端末とサーバとの間の通信及び前記サーバから前記端末へのコンテンツストリームの伝送を行う。

【0043】最初は、モジュール2. 4の権利認証が、前記サーバと対話し始めて、権利認証モジュールの出力

メッセージのような詳細な使用規則と共にコンテンツアクセス及び消費権利を得る。予め決められたフォーマットのこれらのメッセージは、後で使用されるために前記端末のメモリに格納される。出力メッセージ欄を指定する詳細については、後で説明する。

【0044】モジュール2. 4でコンテンツアクセス用権利が許可されると、前記サーバは、前記ネットワーク層を介して要求されたコンテンツストリームを前記端末に送信する。

10 【0045】モジュール2. 2では、他の専用プラットフォーム及びOS用の他のフォーマットに加えてJBC（Java（登録商標）バイトコード）、DLL（ダイナミックリンクライブラリ）などの異なるフォーマットのバイナリツールに加えて、ツールID、ツール位置ID、ツールフォーマットIDを含むツールリスト情報と共にコンテンツストリームを伝送する。ツールリスト情報を指定する詳細については、後で説明する。

20 【0046】モジュール2. 5に示すIPMPツールマネージャでは、ツールリスト情報を構文解析／解釈すると同時に、ツール位置ID及びツールフォーマットID情報に従ってIPMPツールを検索する。モジュール2. 5からの出力メッセージは、ツールの内容を示す記述子用ツールIDを有する適切なIPMPツールである。IPMPツール自体は、IPMP基準で予め決められた共通ツールフォーマットIDに基づいた端末プラットフォーム用に選択し検索して適合するバイナリフォーマットである。

30 【0047】ライセンス／キー及び使用規則は、更なる処理のためにモジュール2. 6のように前記端末のメモリに格納される。対応するツールIDを有するバイナリIPMPツールは、モジュール2. 7のように前記端末のメモリに格納される。前記ツールの各々は、一般的な標準化インタフェースに従って構築され、プラットフォームに適合させる為にコンパイラを用いてプリコンパイルされる。例えば、データ暗号化及び暗号解読のツールは、1つの汎用指定インタフェースに基づいて構築可能である。たとえば、Java（登録商標）仮想マシンで全プラットフォーム／端末用のJava（登録商標）バイトコード（JBC）にプリコンパイル可能であり、またWindows（登録商標）によるプラットフォーム／端末用のダイナミックリンクライブラリ（DLL）にプリコンパイル可能である。

40 【0048】バイナリ形式のツールは、zip形式などの圧縮形式で伝送可能である。前記ツールは、不正変更防止ソフトウェアを用いることにより不正変更可能であり、又は、バイナリコードが破られる又はハッキングされるのを防ぐ署名技法を用いて署名可能である。

50 【0049】モジュール2. 8は、IPMPツールプロバイダ及び端末実施者が予め定めらなければならないIPMPツール用のインタフェースを示す。

【0050】ベース層は、モジュール2.9に示すコンテンツデコーダ及びプレゼンタである。この層は、前記ベース層の他の構成要素に位置して前記構成要素とともにスムーズに動作するバイナリ形式でIPMPツール用のフックインタフェースを用いて構築される。

【0051】汎用インタフェースは、3種類のIPMPツール（暗号解読用インタフェース、透かし埋め込み用インタフェース、透かし技能と暗号解読用インタフェース）について後で明記する。権利認証用インタフェースは、用途に大きく左右されるので予め定義することができず、そのため、ここで定義及び固定されるのではなくパラメトリックツールにより処理される。

【0052】詳細な説明をここで4つの部分に分けて、説明する。

【0053】1. IPMPツールリスト及びIPMPツールマネージャ

1.1 IPMPツールリスト及びIPMPツールマネージャの定義

IPMPの概要において、IPMP情報は、所与のIPMPツールが所与の保護コンテンツを要求して正しく処理する情報と定義されている。IPMPツールは、予め決められた方法で認証、暗号化、透かしなどのIPMP機能を実行するモジュールであると定義されている。

【0054】この発明において、IPMPツールリストの定義を導入する。IPMPツールリストは、IPMPツールマネージャがIPMPツールを識別して前記IPMPツールを検索する必要がある情報を含む。それは、IPMPツールの一意的識別、IPMPツールの位置識別子、及びIPMPツールIDとコンテンツIDとの間の関係定義を含む。

【0055】また、IPMPツールマネージャを次のように定義する。IPMPツールマネージャは、その唯一の役割がIPMPツールリストを処理してコンテンツストリーム全体を消費するのに必要なIPMPツールを検索するエンティティである。

【0056】1.2 IPMPツールリスト

このIPMPツールリストパケットの詳細構造は、次のような図3に最もよく示されている。

【0057】前記IPMPツールリストパケットは、保護コンテンツを消費するのに必要な全IPMPツールの情報を含む。前記コンテンツが2種類以上のコンテンツを含む場合、例えば、前記コンテンツの第1の部分はコンテンツプロバイダAからであり、第2の部分はコンテンツプロバイダBから来ている場合、個々のIPMPツールに関連する情報は、それぞれ関連するコンテンツIDごとに分類される。

【0058】次に、各コンテンツID用のIPMPツールリストは、個々のIPMPツール情報から成れば良く、これらの個々のIPMPツール情報の順序は重要でない。

【0059】各IPMPツール情報は、3つの主要な部分、即ちIPMPツールID、IPMPツール位置識別子及びIPMPフォーマットIDから成る。

【0060】前記IPMPツールIDは、所定の方法でツールを識別し、少なくとも2つの部分、ツールタイプID及びツールサブIDを有する。

【0061】ツールタイプIDは、この特定のIPMPツールが（ツール機能の点から）何れのカテゴリ、例えば暗号解読、透かし抽出、透かし検出、権利抽出などに属するかを指定する。下記の表は、IPMPツールの16カテゴリを扱うことができる4ビットとしてツールタイプIDの長さを仮に設定する。

【0062】更に、ツールサブIDはある特定のIPMPツールを識別し、前記サブIDは、下記の表のように、1ツールタイプ間の4096の異なるツールを識別することができる長さ12ビットとして仮に設定される。

【0063】

【表1】

IPMPツールIDリスト

ツール機能	IPMP ツール ID	IPMP ツール名前	注
暗号解読 ツール	0001 000000000000 ...	DESDecrypt	12ビットに より4096 の異なるツ ールが可能に なる
	0001 000000000001 ...	AESDecrypt	
	0001 000000000010 ...	SC2000Decrypt	
	0001 000000000011 ...	CamelliaDecrypt	
	0001 000000000100 ...	Xxxx	
	0001 000000000101 ...	Xxxx	
	0001 000000000110 ...	Xxxx	
	0001 000000000111 ...	Xxxx	
	0001 000000001000 ...	Xxxx	
	0001 00000000xxxx ...	Xxxx	
	0001 00000000xxxx ...	Xxxx	
	0001 100000000000 ...	予約	今後/独占ツ ールに予約
	0001 100000000001 ...	予約	
透かし埋め 込みツール	0010 000000000000 ...	透かしツール1	12ビットに より4096 の異なるツ ールが可能に なる
	0010 000000000001 ...	透かしツール2	
	0010 000000000010 ...	透かしツール3	
	0010 000000000011 ...	Xxxx	
	0010 000000000100 ...	Xxxx	
	0010 00000000xxxx ...		
			今後/独占ツ ールに予約
		予約	
		予約	

注：上記の最初の4ビットはツールタイプIDである

この表は端末に事前ロードされるべきであり、又は、端
末は上記に示す標準化ツールID表に基づいて構築され
る。

【0064】位置識別子は転送機構を暗示し、1つのI
PMPツールに関して2つ以上の位置識別子が可能であ
る。IPMPツールマネージャは、前記識別子の各々を
用いて前記ツールを検索しようと試みる。IPMPツ
ールAの第1の位置識別子が成功した場合、次の位置識別
子がスキップされ、さもなければ、第2の位置識別子に
続く。例えば、位置識別子は下記の様に記述される。 *

可能な位置タイプとそれらの詳細

位置タイプID	位置タイプ	位置詳細
0000	“ローカル”	N/A
0001	“周辺装置”	N/A
0010	“遠隔ダウンロード可能”	Website(http, ftp...)
0011	“遠隔ダウンロード不可能”	Java servlet などの 遠隔位置
0100	“コンテンツストリーム内部”	この部分はIPMP ツール自体を含むべ きである
...
1***	予約	予約

【0067】ツールフォーマットIDは、IPMPツ
ールID及びツール位置IDと共に伝送され、通知するの
に8ビットを用いており表3に明記されている。

【0068】提供されたIPMPツールが何れのバイナ
リフォーマットであるかをIPMP端末は、DLL、J
BC、又はその他などのツールフォーマットIDから知

- * 1. ローカル：端末システムの内部又は周辺装置
- 2. 外部：指定された端末システムの外部 (http, ftp...)

【0065】IPMPツール識別子は、2つの部分（位
置タイプ及び位置詳細）から成る。位置タイプは、次の
うちの1つでなければならない。位置タイプと位置詳細
との間の対応は、表2に示されている。

【0066】

【表2】

り、前記IPMP端末は、そのOSと合致する適切なフ
ォーマットで前記ツールをダウンロード又は検索でき
る。

【0069】

【表3】

ダウンロードされたIPMPツールのフォーマットID

8ビット	ダウンロードされたフォーマット	対象プラットフォーム	コンパイラ	IPMP端末
00000000	JBC (Java バイトコード)	JVM インタプリタ埋め込みマシン	Java コンパイラ	殆どの携帯電話及びSTBs
00000001	DLL1	Windows マシン	Microsoft C コンパイラ	Windows 上で実行中の全PC
00000010	DLL2	Unix マシン	gcc 及び他のコンパイラ	全 Unix, Linux OS
00000011				
予約	DLL-AM33	パナソニックのチップ	AM33 コンパイラ	チップ依存の製造に予約、及び特定のコンパイラを必要とする
予約				
予約				
予約				

ダウンロードされるIPMPツールのツールフォーマットIDを定義して端末相互運用性を達成する目的は、次の通りである。

1 最近、殆どの携帯電話及びDTV STBは、Java（登録商標）仮想マシン（JVM）で構築されており、ストリーム内の保持又はURLからのダウンロードを介してIPMPツールをJava（登録商標）バイトコードにコンパイルして端末にダウンロードすることができる。

2 DLLは、PC又はUnix（登録商標）で使われる非常に普及しているフォーマットである。異なるビット数のフラグを使用して、ユーザの端末が何れのDLLフォーマットをダウンロードする必要があるかを通知する。

20* 3 JVMも標準C/C++コンパイラも有しない他の端末に関して、例えば、あるDTV STBに、IPMPツールを、それらのコンパイラを用いてプリコンパイルしブロードキャストストリーム又は裏チャンネルを介してダウンロードすることができる。これは、放送業者又は製造業者がそれらのソフトウェアを更新したい時に現在DTV STBが行っていることである。この場合、前記表の同じ予約ビットフラグを、放送業者と製造業者の両方により選択及び参照して、前記業者がIPMPツールの何れのフォーマットを検索して使用することができるかをDTV STBに通知する。

【0070】IPMPツールリスト用構文は、次の通り定義される。

* 【数1】

```

class IPMP_Tool_List
{
    bit(128)          IPMP_Tool_ID;
    //whether this IPMP Tool is a parametric tool or normal to
    ol is implicitly
    // indicated by the IPMP_Tool_ID.
    if (parametricRepresentation)
    {
        //... detailed syntax of parametric representation
    }
    else
    {
        bit(1)hasAlternativeToolLocation;
        while (hasAlternativeToolLocation)
        {
            bit(1)          hasAlternativeToolLocation;

```

```

        bit(7)      Tool_Location_ID;
        if (Tool_Location_ID == 0b00000000) //tool carried
in bitstream.
        {
        }
        else if (Tool_Location_ID == 0b00000001) //remote m
ethod call
        {
        bit(8) Remote_Call_Mechanism; //CORBA, DCOM, RMI, //SOAP ...
            bit(1) Client_In_Bitstream;
        }
        else if (Tool_Location_ID == 0b00000010 || Tool_Location_ID
=0b00000011)
// Remote Downloadable, http protocol or ftp protocol
        {
            bit(8)      Tool_Format_ID;
            unsigned int(16) serverAddressLen;
            bit(8) serverAddress[serverLen];
            unsigned int(16) fullPathLen;
            bit(8) fullPath[fullPathLen];
            bit(1) isCompressed;
            if (isCompressed)
            {
                bit(7) compressionMethod;
            }
        }
        else if (Tool_Location_ID == 0b0000100 .. 0b100000
0) //ISO reserved
        {
        }
        else // user defined.
        {
        }
    }
}

```

【0071】意味

IPMP_Tool_IDは、ユニバーサルレベルでツールを一意に識別する。最初の16ビットは特定のIPMPツールのタイプカテゴリを識別するのに対して、次の112ビットは前記IPMPツールを詳細に識別する。下記の表に、前記IPMP_Tool_IDを説明する。登録当局が、そのような表を保守する責任を持つ。

【0072】幾つかの通常用いられるIPMPツールを標準化する必要があり、それらの基本的なIPMPツールを含むテーブルを定義する必要があり、このテーブルをあらゆるIPMP端末に事前ロードするべきである。下記の表はこの考えを説明する。標準化されるべき基本ツールの内容に関して、それはIPMP委員会で更に論

議する事項である。

【0073】Tool_Location_IDは、転送機構を暗示し、ツールがコンテンツストリームに保持されるか、遠隔位置からダウンロードする必要があるか、又はIPMPツールが遠隔位置で実行可能であるか否かを示す。

【0074】1つのIPMPツールに関して2つ以上の位置識別子が可能である。hasAlternativeToolLocationは、IPMPツールがすべての検索先を有するか否かを示す。IPMPツールマネージャは、前記識別子の各々を用いて前記ツールを検索しようと試みる。IPMPツールAの第1の位置識別子が成功した場合、次の位置識別子がスキップされ、さもなければ、第2の位置識別子が調べられる。

【0075】

* * 【表4】
I PMP ツール位置識別子 (I PMP Tool_Location_ID)

Tool_Location_ID	位置タイプ
000 0000	コンテンツストリーム内に保持されたツール
000 0001	遠隔位置で実行されるツール
000 0010	http プロトコルによるダウンロード
000 0011	ftp プロトコルによるダウンロード
000 0100 -- 100 0000	ISO 予約
100 0001 -- 111 1111	予約

【0076】 Tool_Location_ID が 0 b 0 0 0 0 0 0 0 である場合、それは、I PMP ツールがコンテンツストリームに保持されていることを意味する。Mpeg 4 データにおいて、本発明では、I O D と関連のある提案された I PMP ツール E S 内にバイナリ I PMP ツールを入れる。その詳細は、後で説明する。

【0077】 Tool_Location_ID が 0 b 0 0 0 0 0 0 1 である場合、それは、この I PMP ツールが遠隔側で実行されるものであることを意味し、I PMP 端末は、RPC (遠隔手続き呼び出し) を介してこの I PMP ツールを呼び出す。8 ビット遠隔呼び出し方法は、この I PMP ツールが何れの R P C 機構、例えば CORBA、RMI、XML-RPC、DCOM に対応しているかを示す。この Remote_Call_Mechanism に関する詳細は、下記の表で定義される。I PMP ツールマネージャは、前記端末が前記 R P C 機構に対応しているか否かをチェックする。

【0078】

【表5】

I PMP Remote_Call_Mechanism

Remote_Call_Mechanism	R P C 機構
0000 0000	DCOM
0000 0001	RMI
0000 0010	CORBA
0000 0011	XML-RPC
0000 0100	SOAP
...	...
0000 1000 -- 1000 0000	ISO 予約
1000 0001 -- 1111 1111	予約

【0079】 前記 I PMP ツールが遠隔で実行されるものである場合、I PMP 端末は、遠隔 I PMP ツールとインタフェースをとって通信するクライアントのような軽量コードを必要とする。例えば、前記遠隔 I PMP ツールが CORBA を介して呼び出されることができるだけである場合、前記 I PMP 端末は、I I O P (インターネット O R B 間プロトコル) を介して前記遠隔 I PMP ツールに適切にパラメータをひとまとめに伝達する方法を知っているスタブを必要とする。本発明では、この軽量バイナリコードを I PMP ツールクライアントとし

て呼び出す。I PMP ツールクライアントは軽量であると考えられているので、それは可能であり、コンテンツストリーム内に保持される。この I PMP ツールクライアントをコンテンツストリーム内に保持する方法は、後で説明する。

【0080】 遠隔で実行される I PMP ツールと通信する I PMP ツールクライアントを有するだけでは、I PMP 端末がこの遠隔 I PMP ツールを利用することを可能とするのに十分でない。I PMP 端末は、前記 I PMP ツールクライアントを初期設定してそれに話しかける方法を必要とする。これを処理する方法は、この提案の範囲外である。この面において、I PMP ツールクライアントは他の通常の I PMP ツールと同じように見える。従って、前記 I PMP ツールを丁度他の I PMP ツールのように初期設定して呼び出すべきであり、例えば、I PMP ツールクライアントと I PMP 端末との間のインタフェース定義は、この I PMP ツールクライアントが動作することになっている O D 又は E S D 間の I PMP 記述子に保持されても良い。

【0081】 Tool_Location_ID が 0 b 0 0 0 0 0 1 0 である場合、それは、I PMP ツールマネージャが http プロトコルによって特定の I PMP ツールをダウンロードすべきであることを意味する。0 b 0 0 0 0 0 1 1 は、ftp プロトコルを使用すべきであることを意味する。ServerAddress (例えば、www.panasonic.com) 及び fullpath (例えば、/ipmptools/encryption/tool1.zip) は、この特定の I PMP ツールを検索する場所をはっきりと定義する。I PMP ツールマネージャが http 又は ftp プロトコルを実施して必要な I PMP ツールを検索する方法は、本発明の応用課題である。特定の I PMP ツールを検索するのに使用可能な複数種のプロトコル (https、ssl) がある場合もある。ISO 予約ビット範囲 0 0 0 0 1 0 0 ー 1 0 0 0 0 0 0 は、複数種のプロトコルを保持する様に設計されている。

【0082】 I PMP ツールプロバイダがそれ自身の独占プロトコルを使用したい場合には、ビット範囲 1 0 0

0001-11111111を使用すれば良い。

【0083】IsCompressedビットは、指定ツールが圧縮されているか否かのフラグを立てる。圧縮されている場合、IPMPツールマネージャは、compressionMethod欄に明示の圧縮方法に従って前記ツールを伸張する必要がある。PC用圧縮方法は多数あり、とりわけPKZip、LHARc、ARJ、及びZOOがある。マッキントッシュでは、StuffIt、CompactPro及びその他がある。複数の圧縮方法をIPMPで使用できる様にすることもでき、又は1つの圧縮方法をデフォルトとして指定することもできる。

【0084】IPMP_ToolES

Mpeg4システムのデータにおいて、本発明では、基*

IPMP Remote_Call_Mechanism

ストリームタイプ値	ストリームタイプ記述
0x00	禁止
0x01	ObjectDescriptorStream (ISO/IEC 14496-1 参照)
0x02	ClockReferenceStream (ISO/IEC 14496-1 参照)
0x03	SceneDescriptionStream (ISO/IEC 14496-1 参照)
0x04	VisualStream
0x05	AudioStream
0x06	MPEG7Stream
0x07	IPMPStream (ISO/IEC 14496-1 参照)
0x08	ObjectContentInfoStream (ISO/IEC 14496-1 参照)
0x09	MPEGJStream
0x0A	IPMPToolStream
0x0B-0x1F	ISO 使用に予約
0x20-0x3F	ユーザ専用

【0087】前記IPMPToolStreamを復号するデコーダは、IPMPツールマネージャである。0x0Aのストリームタイプを参照する際に、IPMP端末は、構文解析するIPMPツールマネージャに前記基本ストリームを渡す。IPMPToolStream ※

```

class IPMP_ToolES
{
    IPMP_Tool ipmp_tools[0 .. 255];
}

class IPMP_Tool
{
    bit(128) IPMP_Tool_ID;
    bit(8) Tool_Format_ID;
    bit(1) isCompressed;
    if (isCompressed)
    {
        bit(7) compressionMethod;
    }

    bit(1) isSigned;
    if (isSigned)
    {
        bit(8) signature_Algorithm[];
        bit(8) signature_Parameters[];
    }
}

```

* 本ストリーム間に（前記で提案したIPMPツールクライアントを含む）バイナリIPMPツールを保持する。その目的を果たすために、本発明では、基本ストリームに対応付けられたデコーダ構成記述子に新しいストリームタイプを定義する。

【0085】ストリームタイプ“IPMPToolStream”を以下の様に、提案する。0x0A-0x1FがISO使用のために予約されているので、このストリームタイプに割当てられる値を0x0Aと設定する。従って、Mpeg4システム仕様の現バージョンで定義されたストリームタイプ表を、下記のように変更する。

【0086】

【表6】

※は、初期オブジェクト・デスク립タODに通常置かれている。

【0088】IPMP_ToolESの構文

【数2】


```

bit(1) IPMP_Tool_List_Signature[];
}
bit(16) Tool_Size;
bit(Tool_Size) Tool_Body;
}

```

【0089】IPMP_Tool_List_Signatureの意味

IPMP_Tool_List_ID、Tool_Format_IDは、前記で定義されている内容と同じ意味を有する。

【0090】前記基本ストリームに保持されたIPMP_Tool_Listは、IPMP_Tool_Listの安全性を保証するためにある特定の署名アルゴリズムを用いて署名可能である。

【0091】前記署名の確認後、IPMPツールマネージャは、Tool_Sizeにより指定されたサイズのTool_Bodyをハードディスク又は物理メモリに適切に格納する。前記端末又はメッセージルータは、そのことを認識している。

【0092】前記IPMP_Tool_List_Streamに保持可能なIPMPツールは、提案したIPMPツールクライアントを含む。基本ストリームからの検索及びIPMP端末による初期設定の後、IPMPツールクライアントは、遠隔IPMPツールと対話する。しかし、前記端末にとって、前記IPMPツールクライアントは、一意のIPMP_Tool_List_IDを有する通常のIPMPツールとあまり変わらない。

【0093】1.3 IPMPツールマネージャ

IPMPツールマネージャは、システムのデマルチプレクサの前又は後に位置することができる。その機能性は、コンテンツストリーム内にあるIPMPツールリストを構文解析することである。

【0094】図4に示す線図は、IPMPツールマネージャがMpeg4-IPMPシステムに組み込まれた例を示す。

【0095】IPMPツールマネージャは、次の4つのステップを実行する。

・ステップ1：入力IPMPデータをIPMPツールリストを求めて構文解析する。前記リストがない場合、ステップ4に進み、他の場合、正規の構文に従って前記IPMPツールリスト間のIPMPツール情報を構文解析する。

・ステップ2：すべての要求IPMPツールが端末に入手できる場合、ステップ4に進む。

・ステップ3：IPMPツール情報で指定された必要なIPMPツールを検索し、検索が成功しない場合、中止し、他の場合、ステップ4に進む。

・ステップ4：全IPMPツールをうまく取得した後、アクセス許可がある場合、利用可能なコンテンツは、データバッファに流れ始めることが可能となる。

【0096】コンテンツストリームを受信する際に、I

MPMPツールマネージャは、あらゆるコンテンツストリームに関する一意のヘッダであるIPMPツールリストパケットフラグを捜すことにより前記コンテンツストリームをまず調べる。IPMPツール情報パケットの前記フラグが見つからない場合、ステップ4にジャンプする。

【0097】第3のステップにおいて、IPMPツールマネージャは、位置識別子タイプID及び位置識別子詳細を調べることにより各IPMPツールを検索しようと試みる。1つのIPMPツールに対応付けられた2つ以上の位置識別子がある場合、前記IPMPツールマネージャは、まず位置識別子1を用いて前記IPMPツールを検索しようと試み、それが失敗した場合、次に位置識別子2を用いて検索しようと試みる。

【0098】位置識別子タイプが「ローカル」の場合、IPMPツールマネージャは、指定されたIPMPツール名前又はIPMPツールIDに従って端末自身の中を探索する。

【0099】位置識別子タイプが「周辺装置」の場合、IPMPツールマネージャは、指定されたIPMPツール名前又はIPMPツールIDに従ってすべての周辺装置を探索する。

【0100】位置識別子タイプが「遠隔ダウンロード可能」の場合、IPMPツールマネージャは、指定された遠隔アドレスに接続し、必要ならば、相互に受入れ可能な通信チャンネルをIPMPツールマネージャとツールプロバイダとの間にセットアップする。位置識別子タイプが「遠隔ダウンロード不可能」の場合、IPMPツールマネージャは、前記遠隔アドレスをIPMPシステムに渡すだけである。

【0101】位置識別子タイプが「コンテンツストリーム内部」の場合、IPMPツールマネージャは、ツールフォーマットIDをチェックすることにより端末に適合するバイナリフォーマットで前記ツールをロードし、ツール記述子として格納されたツールエンティティにIPMPツールIDを割当てる。

【0102】デマルチプレクサイントーフエス304の後に、音声デコーダバッファ306、映像デコーダバッファ307、IPMPツールデコーダバッファ301、オブジェクトディスクリプタデコーダバッファ308、バイナリデータフォアシーン (binary data for scene) (BIFS) デコーダバッファ309、IPMPデコーダバッファ310が含まれる。バイナリデータフォアシーンは、セグメント化されたシーンの配置場所を示すデータが含まれる。306、307、309の出力である、音

声信号、映像信号、BIFS信号はまだ暗号化されたままの状態である。メモリ302にはツールA（一つ、又は複数）が各端末に予めインストールされている。

【0103】音声デコーダバッファ306は制御ポイント331を介して音声復号311に接続され、映像デコーダバッファ307は制御ポイント332を介して映像復号312に接続され、オブジェクトディスクリプタデコーダバッファ308は、そのままオブジェクトディスクリプタ復号313に接続され、バイナリデータフォアシーン（binary data for scene）（BIFS）デコーダバッファ309は制御ポイント333を介してBISF復号314に接続される。また、IPMPデコーダバッファ310は、IPMPメッセージルータ324のIPMPエレメンタリestream325に接続される。IPMPエレメンタリestream325には暗号化されたスクランブルキーが保持されている。

【0104】図において、黒丸で示された制御ポイント331～339は、IPMP制御ポイントであり、制御ポイントを通過するデータは、IPMPシステム324にあるツールを利用して、必要な処理（デスクランブル、透かし検出、コピーガード等）が加えられる。

【0105】この実施の形態では、制御ポイント331、332、333ではデスクランブルが行なわれる。デスクランブルに必要なツール（ソフト）は、IPMPメッセージルータ324、端末ツールメッセージインターフェース321を介してIPMPツール1、2、又は3から取得する。

【0106】音声復号311は、制御ポイント334を介して音声コンポジットバッファ315に接続され、映像復号312は、制御ポイント335を介して映像コンポジットバッファ316に接続され、BIFS復号314は、制御ポイント336を介して復号BIFS317に接続される。

【0107】制御ポイント334、335、336では透かし検出が行なわれる。透かし検出に必要なツール（ソフト）は、IPMPメッセージルータ324、端末ツールメッセージインターフェース321を介してIPMPツール1、2、又は3から取得する。例えば、IPMPツール2は、デスクランブルに必要なツールが保持されており、IPMPツール3は、透かし検出に必要なツールが保持されている。音声コンポジットバッファ315は、制御ポイント337を介して合成器318に接続され、映像コンポジットバッファ316は、制御ポイント338を介して

```

Class      UserAuthentication( )
{
Class      ReceivingContentStream( )
{
Class      DemuxContent( )
{
Class      IPMPToolsManagement( )

```

*して合成器318に接続され、復号BIFS317は、制御ポイント339とBIFSツリー319を介して合成器318に接続される。合成器318は更に出力であるレンダリング320に接続される。

【0108】制御ポイント337、338、339では別の透かし検出や、コピーガード処理が行なわれる。透かし検出やコピーガード処理に必要なツール（ソフト）は、IPMPメッセージルータ324、端末ツールメッセージインターフェース321を介してIPMPツール1、2、又は3から取得する。

【0109】IPMPツールマネージャ300は、IPMPツールリストを解析する解析部350と、IPMPツールを検索する検索部351がある。オブジェクトディスクリプタデコーダバッファ308は、そのままオブジェクトディスクリプタ復号313に接続され、コンテンツストリームに含まれるオブジェクトディスクリプタを復号する。復号されたオブジェクトディスクリプタは、IPMPツールマネージャ300に送られ、必要とされるツールが存在する位置について特定がなされ、そのツールを取得するためのデータがIPMPツールマネージャ300からツールメッセージインターフェース321に送られる。ツールメッセージインターフェース321は、特定されたツールがメモリ302にあればそのツールをIPMPツール2または3に移動し、必要な処理を行なう。特定されたツールがメモリ302にない場合は、インターネットなどの伝送路を介し、リモートツール360にアクセスし、必要なツールをIPMPツール1にダウンロードする。また、必要なツールが遠隔IPMPツールB362にしかなく、ダウンロードが出来ない場合は、暗号化されたデータをそのまま、IPMPツールBのローカルクライアント364を介して遠隔IPMPツールB362に送り、遠隔IPMPツールB362で解読したデータを送り返す様に動作する。

【0110】IPMPツールマネージャ及びIPMPツールリストを含むこのアーキテクチャは、任意のMPEG-nシステムに適用でき、図5は、IPMPツールマネージャがMPEG2-IPMPシステムに組み込まれる場合を示す。ここに示す例では、オブジェクトが含まれない。PESで示される黒丸で示す制御ポイントにおいてデスクランブルや、透かし情報の解読が行なわれる。

【0111】コンテンツの同一部分に対しては、MPEG-nのIPMPシステムに関する一般的な構文は、次のような流れで定義可能である。

【数3】

【表 8】

バイナリフォーマットで定義された消費タイプ及び規則

消費タイプ	8 ビット	消費規則タイプ 4 ビット+変数	注
アクセス	00000000		アクセスコンテンツ
プレー (ストリーミング)	00000001		ストリーミング再生
格納及びプレー	00000010		格納及び再生
		0001+ プレーカウント	
		0010+ プレー時間	
		0011+ プレー期間	
		0100+コピーカウント	
		0101+移動カウント	
シーングラフ編集	00000011		
時間ライン編集	00000100		
テキスト又はその他の追加			
	予約		

【0120】図6に示す線図は、MPEG-4のIPMPシステムと共に作動するユーザ認証モジュールを示し、ユーザ認証の実行後にコンテンツエージェントを要求してライセンスをユーザに発行する。ユーザID情報は、IPMPシステム内に含まれている。このユーザID情報が標準では定義しないユーザ認証においてユーザIDの照合が行なわれる。この照合には例えば乱数が用いられる。照合が成立すれば、正しいユーザとしてサーバに対しユーザ登録を行なう。

【0121】図7の線図に示すように、2重セキュリティ構造は、MPEG-nのIPMPに関して実現可能である。サーバから送られてきたライセンスキーは、IPMPツール保持部に送られる。また、コンテンツストリームに含まれる暗号化されたスクランブルキーが点線で示す経路を経て、IPMPツール保持部に送られる。IPMPツール保持部では、ライセンスキーを用いてスクランブルキーの解読を行なう。解読されたスクランブルキーは、スクランブルキー保持部で保持され、IPMPツールの動作に使用される。この様に、IPMPツールは、スクランブルキーとライセンスキーによる2重のセキュリティがかかっている。

【0122】3. IPMPツール用の一般的なインタフェース

データ暗号化/暗号解読、透かし、及び結合透かし及び暗号解読を使用する典型的な用途シナリオを我々が設定した場合、汎用のインタフェースを定義することができる。

【0123】データ検出インタフェース

ブロックベースデータ暗号化/暗号解読ツールは、独自のIPMPシステムにおいてより重要でより広く使用され、特にそのアルゴリズムはある種の収束性を有することが知られている。そこで、そのインタフェースをうまく指定してデータ暗号化及び暗号解読技法の殆どを表す

ことができ、前記技法の一部は知られていないが、そのインタフェースは予測範囲内である。

【0124】データ暗号化/暗号解読の対称アルゴリズム用のNESSIEインタフェースあらゆるアクセスユニットのブロックベースデータ暗号化/暗号解読用の汎用インタフェースは、IPMPシステムで定義可能である。IPMPツールプロバイダとIPMP端末実施者の両方は、同一のインタフェースに従って、ツールプロバイダ側でツールをバイナリフォーマットにコンパイルし、IPMP端末側に正しいバイナリツールを伝達することができる。下記のインタフェースは、NESSIE（署名、保全性及び暗号化に関する新欧州方式）で定義されており、我々は、ブロックデータ暗号化/暗号解読用に我々が定義したIPMPシステムで前記インタフェースに適合することができる。前記インタフェースは、下記のように示され、3種類、NESSIEkeysetup()、NESSIEencrypt()及びNESSIEdecrypt()から成る。

【0125】void NESSIEkeysetup(const unsigned char * const key, struct NESSIEstruct* const structpointer);

void NESSIEencrypt(const struct NESSIEstruct * const structpointer, const unsigned char * const plaintext, unsigned char * const ciphertext);

void NESSIEdecrypt(const struct NESSIEstruct * const structpointer, const unsigned char * const ciphertext, unsigned char * const plaintext);

【0126】透かしインタフェース

透かしを使用する目的に関して、4つの主な分野がある。

・著作権保護—メディアデータの正当な所有権を決定する。

・違法コピー追跡—違法製造コピーを監視して追跡す

る。

・コピー保護—メディアの許可されていないコピーを禁止する。

・画像認証—データの改造を検出する。

【0127】前記分野の各々を分析することにより、次のような事が分かる。著作権保護の場合、符号化側で埋め込みを行い、オフラインで検出を行う。そこでは、他のリアルタイム暗号解読及び復号モジュールと共にI PMP端末で実時間実施される必要はない。

【0128】コピー保護の場合には、透かしの使用よりも権利認証ツールの方がずっと複雑な使用規則を提供できるので、よりうまく処理可能である。

【0129】コンテンツ暗号化及び復号を制御する透かしを使用する場合、透かし検出器は、I PMP端末で指定して実装する必要がある。

【0130】たとえ透かしコピー制御埋め込み及び検出にどんなアルゴリズムを使用しても、透かし検出用の汎用インタフェースは、次の通り準拠I PMP端末に関して指定可能である。

【0131】PSL透かし検出(Unsigned Char* Input, 20
Unsigned Char* WatermarkInfor)コピー制御をコンテンツプロバイダ/ディストリビュータ側で埋め込み、暗号化及び復号後にコピー制御検出を行うので、上記インタフェースを、I PMP端末で指定して実装することで、異なる透かし検出技法をもI PMP端末で使用可能にする必要がある。

【0132】画像認証に関して、この場合は著作権保護と同様である。それは、オフラインで行うことができる。

【0133】違法コピー追跡用には、他のシステムで広く提案され使用されているコンテンツ追跡の目的でユーザID又は端末IDを埋め込む透かし埋め込みは優れた機能である。また、基本的な特徴として透かし埋め込みを使用することをここで提案し、I PMPシステムに格納されたり再生用途でコンテンツが違法にコピーされるのを更に防ぐ。ここでI PMPシステムでは、良く知られているように、最初は保護がデータ暗号化/暗号解読を介して行われ、違法コピーに関する追跡が透かし埋め込みを介して行われる。

【0134】たとえ透かし埋め込み、空間定義域又は周波数定義域にどんな技術を使用しても、たとえそれらをどんな分野、映像又は音声に使用しても、入力メッセージ及び出力メッセージは同一であるべきであり、それは次の通りである。

PSLWatermarkEmbedding (Unsigned Char* Input, Unsigned Char* WatermarkInfor, Unsigned Char* Output)

【0135】この場合、透かしの検出をオフラインで行うことができる。

【0136】どんな種類のアルゴリズムがユーザID又は端末IDの透かし埋め込みに使用されるかに関して 50

は、I PMP端末実施者の責任である。この場合、準拠I PMP端末が透かし埋め込み機能を実施してID又は端末IDを埋め込み違法コピーを追跡する必要があるI PMPシステムで要件を設定する限り、前記インタフェースは、I PMPシステムで指定する必要さえもない。

【0137】I PMP端末で使用された独立型透かしに関する結論では、汎用インタフェースは透かしを用いたコピー制御検出の場合にのみ定義される。

【0138】結合透かし検出及びデータ暗号解読 10
コンテンツに埋め込まれる暗号解読用キーは、キー自体を処理することによりコンテンツを保護する優れた方法である。このような場合、2つのインタフェースを次の通り指定可能である。

PSLWatermarkExtraction (Unsigned Char* Input, Unsigned Char* Key)

PSLDecryption (Unsigned Char* Input, Unsigned Char* Key, Unsigned Char* Output)

【0139】処理は、下記のものである。AU用コンテンツ復号→キー抽出→前述のAUで抽出されたキーを用いた次のAU暗号解読、循環規則で実行可能である。

【0140】4. 部分的データ暗号解読

図8では、データ暗号化及び暗号解読をビットストリーム全体ではなくビットに適用して選択することができることを示している。

【0141】図8(a)では、エンコーダを有する部分的暗号化を示しており、コンテンツプロバイダ側で符号化処理中に重要なビットに関して暗号化を選択的に実行できることを説明する。

【0142】図8(a)において、モジュール8. 1 30
は、MPEG2、MPEG4などに基づいて音声又は映像などの元の入力源をストリームに符号化するエンコーダである。モジュール8. 2では、選択されたビット又は情報が他のビットの中で必須又は重要であるため、これらのビット又は情報を暗号化してコンテンツを保護する。8. 0はスイッチであり、8. 8はスイッチ8. 0を切りかえるセクタである。図8(a)では、セクタ8. 8は予め決められた周期または時間区分により切り替え信号を出力する。これにより、エンコーダの出力は決められた時間区分において暗号化がかけられ、他の時間は暗号化がなされない。

【0143】図8(b)では、エンコーダでエンコードされたデータの内、暗号化を重要なビットに関して選択的に実行できる例を示す。なお、エンコーダ8. 1はコンテンツディストリビュータの中にある場合だけでなく、コンテンツディストリビュータの外にある場合も含む。後者の場合であれば、コンテンツディストリビュータは、エンコードされたストリームを受け、それを配信する。これは、コンテンツディストリビュータが既存又はそれら自体の暗号化ツールを用いて符号化コンテンツを保護したい場合である。

【0144】図8(b)において、モジュール8.3は、モジュール8.4で実行される暗号化用の重要なビットを構文解析して選択するセクタを有する部分的デコーダである。エンコードされたストリームは、そのままスイッチ8.0に送られると共に、部分的デコーダおよびセクタ8.3にも送られる。部分的デコーダおよびセクタ8.3は、エンコードされたデータをデコードし、重要なデータ部分、たとえば映像信号の場合、I-ピクチャーの部分やP-ピクチャーの部分を検出する。そして、重要なデータ部分が検出された時に、その部分に対応するエンコードストリームの区分を暗号器8.4に送る様にスイッチ8.0を動作する。このため、エンコード8.1からの分岐点とスイッチ8.0との間に必要な遅延部を設けても良い。部分的デコーダおよびセクタ8.3は、入力されるエンコードされた信号を部分的にデコードしても良いし、全体をデコードしても良い。

【0145】図8(c)は、デコード側の構成を示す。ここでは、部分的暗号解読が示されている。IPMP端末側で生じる、部分的暗号化ストリームの暗号解読を選択的に実行する実施の形態を示す。

【0146】図8(c)において、モジュール8.5は、モジュール8.6で実行される暗号解読用のビットを構文解析して検出する検出器を有する部分的デコーダである。同時に、復号された音又は画像は、モジュール8.7から出力される。検出器8.5は、デコードを試みることにより、デコードが可能な部分と不可能な部分を検出する。不可能な部分については、その部分に相当するストリームは暗号化されている区分であると判断し、暗号化されている区分を検出する。ストリームの内暗号化されている区分は暗号解読器8.6に送られ、暗号が解読される。

* 【表9】

異なる端末用の3つのプロファイル

プロファイル	IPMP ツール取得	
	事前符号化	ダウンロード済み
単純プロファイル 固定 IPMP ツール	あり	なし
コアプロファイル 柔軟 IPMP ツール及び固定インタフェース	あり	あり
高プロファイル 柔軟 IPMP ツール及びインタフェース	あり	あり、より多くのツールを支援できる

【0152】ツールが固定される場合は、標準の方法で勧められるIPMPツールの種類を定義して製造者が端末に実装可能にする必要がある。この場合、インタフェースは、IPMP端末実装者により決定される。

【0153】ツールは固定されないがインタフェースが固定される場合に関して、標準の方法で異種のIPMPツールに関する幾つかの汎用インタフェースを指定する必要がある。

* 【0147】5. IPMPシステム用の可能なプロファイル

異なるアプリケーション、異なる端末、異なるベンダは、IPMPシステムに関する異なる要件を有し、たった1つの基準で全部を扱うことは困難である。基本的に、この課題は、IPMPツールが事前ロードされるか、又はダウンロード可能であるかに依存する。単純なハードウェア実現に関しては、多くの場合がJava（登録商標）仮想マシンを装備しているのである特定のツールがダウンロード可能であるセットトップボックスの新プラットフォームやモバイル装置でさえ多くの場合、殆どのツールは事前ロードされるか、又は組み込まれる。

【0148】複雑さの少ない実施を要求する場合にはので、あるモバイル又はポータブル端末は事前符号化IPMPツールを有する必要がある。PCアプリケーションは非常に柔軟であり、ツールは、ダウンロード可能又は事前符号化されていてもよい。

【0149】IPMPツールがダウンロード出来る場合、ダウンロードされたIPMPツールのインタフェースも、定義される必要がある。メッセージインタフェースは、未知又は専用IPMPツールを処理するIPMP端末に高い柔軟構造を与える優れた解決策であるが、IPMP端末に対してより複雑な実装を要求する。

【0150】3つのプロファイルを指定する場合、表5に示すように端末機能に基づいて3つの場合を扱う。すなわち、固定IPMPツール用の単純プロファイル、柔軟IPMPツール及び固定インタフェース用のコアプロファイル、並びに柔軟IPMPツール及び柔軟インタフェース用の高プロファイルの3つである。

【0151】

* 【表9】

【0154】ツールとインタフェースの両方が固定されない場合に関して、メッセージインタフェースを詳細に指定して標準の方法で動作を通知する必要がある。

【0155】この発明は、IPMPツールリストを構文解析してIPMPツールを取得するIPMPツールマネージャモジュールと共にコンテンツストリームの前のIPMPツールリストパッケージを取り入れることにより異種のIPMPシステムにより同一の保護コンテンツを再

生する課題を解決する。IPMPツールフォーマットIDを指定することにより、異なるフォーマットのIPMPツールをダウンロードしてIPMP端末に一致させることができる。更に、3つの主要なIPMPツール用の一般的なツールインタフェースも、この発明で指定してIPMPシステムを完全にする。

【0156】2層構造は、より高いセキュリティを与えるだけでなく、異なるユーザ認証方法用の出力構造も固定して、端末互換性を持たせる。このような構造では、ユーザ認証を異なるベンダに関して異なる方法で実施して、相互運用性を確保することができる。

【0157】異なるプロファイルは、IPMPツールを取得して使用する端末複雑性及び柔軟性を考慮して定義され、異なる端末及び異なるIPMPツールベンダに関して広範囲の適用を与えてながら同一の標準を使用することを可能にする。

【0158】図9は、他の実施の一例における著作権保護システムの構成図である。図9において、1はプロバイダ、2はユーザ端末、3はネットワークであり、プロバイダ1とユーザ端末2を接続している。プロバイダ1は、暗号化コンテンツ11と、その解読鍵12、及び、著作権保護ツールの一つである解読モジュール13と、著作権保護情報の一つであるコンテンツの利用規則14と、その利用規則を管理する著作権保護ツールの一つである利用規則管理モジュール15を持ち、ユーザ端末2は、初期状態としてなにも持っていない。以上のように構成された本発明の一実施例における著作権保護(IPMP)システムにおいて、著作権保護システムを更新し、暗号化コンテンツを利用規則に従って解読、再生する方法を以下に述べる。

【0159】図10は、本発明の実施例における著作権保護システムにおいて、プロバイダとユーザ端末の間で交換するメッセージの流れを示す図である。図11は、メッセージの具体例であり、各メッセージは、「=」記号の左辺に示す予め登録されているメッセージ項目名と、「=」に続くメッセージ項目の値(データ)の組で構成される。

【0160】まず、ユーザ端末2は、視聴したいコンテンツを持つプロバイダにユーザ登録をして必要な著作権保護(IPMP)ツールを入手するためにメッセージ1をプロバイダ1へ送る。メッセージ1は、メッセージ項目として、メッセージID(識別子)、ユーザ名、支払い方法、及び、ユーザ端末情報より構成される。各メッセージ項目の値は以下である。メッセージ1の目的は、ユーザ登録である為、メッセージIDの値は「ユーザ登録」を表わす値であり、登録に必要なユーザ名の値は、「松下

太郎」である。又、視聴するコンテンツの対価の支払い方法の値は、ユーザのクレジットカードの種類、番号、有効期限を含む暗号化された「クレジットカード番号」である。ユーザ端末情報の値は、Windows(登録商

標) OS上で動くマシンであるので「Windows(登録商標) OS」である。これらの情報は、ネットワーク3の入り口で更に暗号化され、出口でその暗号が解読される。暗号の方法は、公開鍵暗号方式や共通鍵暗号方式が用いられるが、この内容は、例えば、岡本他「現代暗号」産業図書、1997年に詳述されている。

【0161】メッセージ1を受け取ったプロバイダは、ユーザ名、解読されたクレジット番号を記録し、ユーザID「XYZ」をユーザ端末2に割り当て、ユーザ端末2にメッセージ2を返す。メッセージ2は、ユーザがコンテンツを視聴するために必要な初期設定を行うもので、メッセージIDの値は、「初期設定」であり、ユーザIDの値「XYZ」と、プロバイダが持っているコンテンツの一覧表である「コンテンツリスト」をIPMP情報の値として含み、又、暗号化コンテンツを解読する為の解読モジュールの識別子(解読モジュールID)と、その存在する場所(ロケーション)を、IPMPツール情報の値として含む。更に、コンテンツを利用規則に従って視聴させる為、利用規則管理モジュールの識別子(利用規則管理モジュールID)とその存在する場所(ロケーション)をIPMPツール情報の値として含む。このとき、解読モジュールと利用規則管理モジュールは、Windows(登録商標)マシンであるユーザ端末に直接組み込めるものが選ばれる。メッセージ2も、以降のメッセージも、ネットワーク3を通過する際に暗号化されることは、言うまでもない。

【0162】メッセージ2を受け取ったユーザ端末は、解読モジュールIDとそのロケーションで指定される解読モジュールと、同じく利用規則管理モジュールIDとそのロケーションで指定される利用規則管理モジュールを、ファイル転送などの手段で入手し、自身に著作権保護ツール(IPMPツール)として組み込む。このファイル転送も又、暗号化されたファイル転送であり、他のユーザ端末は暗号解読の鍵を持たない為、モジュールを傍受したとしても解読できない。次に、ユーザ端末2は、コンテンツリストから視聴を希望するコンテンツ1を選び、コンテンツ要求をメッセージIDとして持つメッセージ3をプロバイダに送る。メッセージ3は、更に、ユーザIDとして値「XYZ」を含み、コンテンツ情報として要求するコンテンツ1のIDを含む。

【0163】これを受けたプロバイダ1は、要求されたコンテンツ1の対価を、ユーザのクレジットカード番号を使ってクレジットカード会社に請求した後、暗号化コンテンツ1をユーザ端末2に送る為、メッセージ4を返す。メッセージ4は、メッセージIDと、2つの著作権保護(IPMP)情報、及びコンテンツ情報で構成される。メッセージIDの値は「コンテンツ配信」であり、IPMP情報の値は、要求されたコンテンツ1の利用規則1と、暗号化されたコンテンツ1の暗号を解く為の解読鍵1である。コンテンツ情報は、要求された暗号化コンテンツ1そのものである。解読鍵1は、公開鍵暗号方式で暗号化

されてユーザ端末2に送られるので、このメッセージ4を第三者が傍受しても解読鍵の暗号を解読出来ず、コンテンツの漏洩は起こらない。

【0164】メッセージ4を受け取ったユーザ端末2では、先ほど組み込んだ利用規則管理モジュール25が、利用規則1を確認しながら、解読モジュール23を制御し、解読モジュール23は、解読鍵1を使って、暗号化コンテンツ1を解読し、解読されたコンテンツ1を表示出力する。解読モジュール23が暗号化コンテンツ1の暗号を解く動作は、共通鍵暗号方式であり、上述の文
10

【0165】次に、図12に示す利用規則1の一実施例に従い、暗号化コンテンツ1の解読を行う解読モジュール23を制御する利用規則管理モジュール25の動作を、図13のフロー図を用いて以下に説明する。

【0166】まず、利用規則管理モジュール25は、利用規則1の第1行目を調べ、このコンテンツが利用可能期間内に入っているか否かを、ユーザ端末の持つ時計で確認し、入っていない場合は、処理を終了する。入っていれば次に、ユーザにこのコンテンツを別メモリに移動するか
20

【0167】次に、ユーザにこのコンテンツのコピーを作るか否かを確認し、作る場合は、利用規則1内のコピー可能回数を調べ、この値がゼロより大であれば、ユーザの指定するメモリにコンテンツとその利用規則をコピーし、コピー可能回数を1減じる。コピー先のコンテンツのコピー可能回数は、処理の簡単化のためにゼロとするが、トータルのコピー回数が初期のコピー可能回数を
30

【0168】次に、ユーザにこのコンテンツを再生するか否かを確認し、再生する場合は、利用規則1内の再生可能回数を調べ、この値がゼロより大であれば、解読モジュール23にコンテンツの解読・表示出力を指令する。指令を受けた解読モジュール23は、コンテンツ1の暗号解読を行いその結果を表示出力することは上述の通りである。

【0169】次に、利用規則管理モジュール25は、再生終了を検出し、それまでに再生した時間が無料再生時間を超過したか否かを調べ、超過した場合は、再生可能回数を1減じて終了する。

【0170】以上に述べた利用規則管理モジュール25による利用規則1の管理により、プロバイダ1が意図した回数の再生のみが実行される。同時に、コピー回数や、移動回数もプロバイダの意図どおりに管理される。尚、本実施例では、メッセージは、予め決められたメッセージ項目と「=」で結ばれたその項目の値（データ）との組で構成されていたが、メッセージの値の意味が分
50

かる方法であれば何でも良く、例えば、メッセージ中のビットの位置に予め決められた意味を割り当てる方法でも良い。

【0171】以上のような構成及び方法により、本発明の更新可能な著作権保護システムでは、プロバイダからユーザ端末に送られるメッセージをユーザ端末が解読することにより、著作権保護モジュールの更新と、プロバイダが与える利用規則に従ったコンテンツの視聴が可能となる。すなわち、メッセージ中にモジュールIDが存在する
10

【図面の簡単な説明】

【図1】 先行技術のコンテンツ提供及び保護の既存IPMPシステムを示す。

【図2】 準拠IPMPシステムの一般図を示す。

【図3】 コンテンツストリームに保持されたIPMPツールリストパケットの構成を示す。

【図4】 MPEG-4のIPMPシステムと共に作動するIPMPツールマネージャの構成を示す。

【図5】 MPEG-2のシステムと共に作動するIPMPツールマネージャの構成を示す。

【図6】 MPEG-4のIPMPシステム及びIPMPツールマネージャモジュールと共に作動するユーザ認証モジュールの構成を示す。

【図7】 MPEG-2のシステム及びIPMPツールマネージャモジュールと共に作動するユーザ認証モジュールの構成を示す。

【図8】 (a)はエンコーダを有する部分的暗号化の構成を示し、(b)はエンコーダを有しない部分的暗号化の構成を示し、(c)は部分的暗号解読の構成を示す。

【図9】 本発明の他の実施例のIPMPシステムの構成図を示す。

【図10】 本発明の実施の形態におけるIPMPシステムにおいて、プロバイダからユーザ端末に送られるメッセージの流れ図を示す。

【図11】 メッセージの具体例を示す。

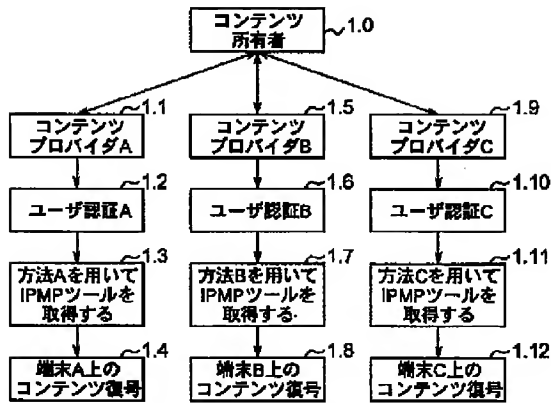
【図12】 メッセージ内のIPMP情報の一例を示す。

【図13】 利用規則管理モジュールの処理フロー図を示す。

【符号の説明】

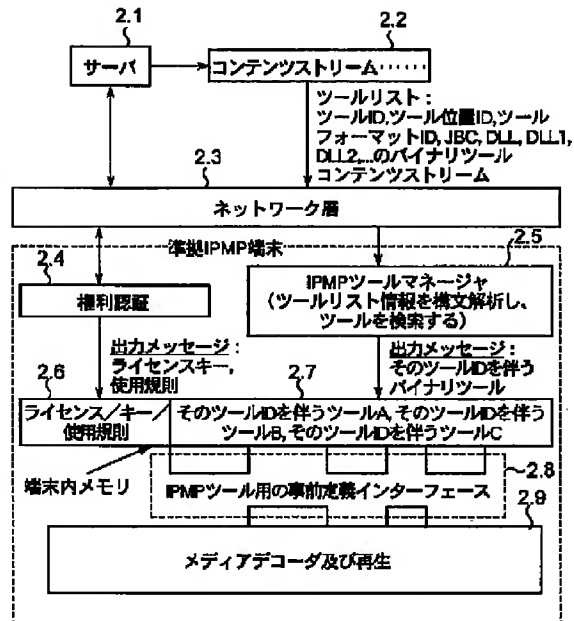
- 2. 1 サーバ
- 2. 2 コンテンツストリーム
- 2. 3 ネットワーク層
- 2. 4 権利認証

【図1】

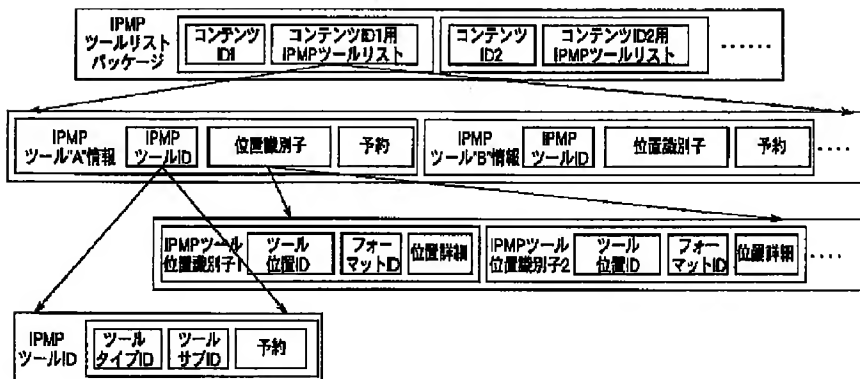


- * 2. 5 IPMPツールマネージャ
- 2. 6 ライセンス/キー/使用規則
- 2. 7 メモリ
- 2. 8 IPMPツール用の予め定めたインタフェース
- * 2. 9 メディアデコーダ及び再生装置

【図2】



【図3】

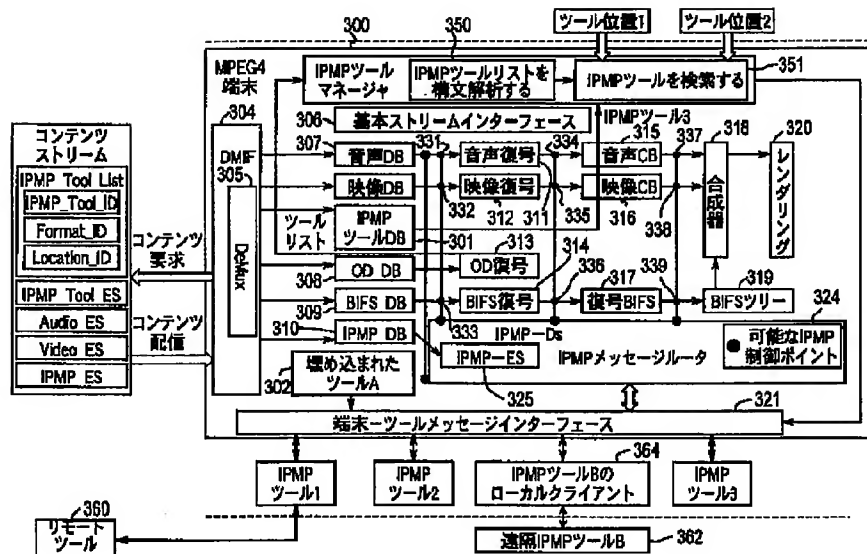


【図12】

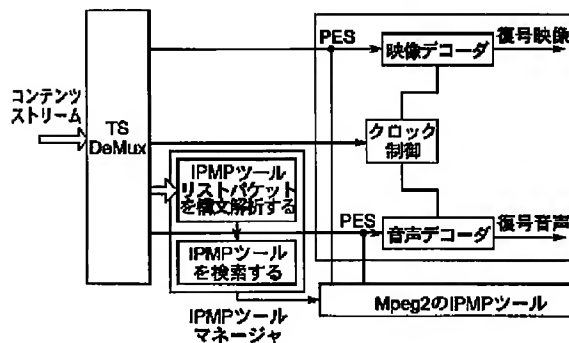
利用規則1

利用可能期間=	2001.6.1-2001.6.30
無料再生時間=	1分
再生可能回数=	3
コピー可能回数=	1
移動可能回数=	5

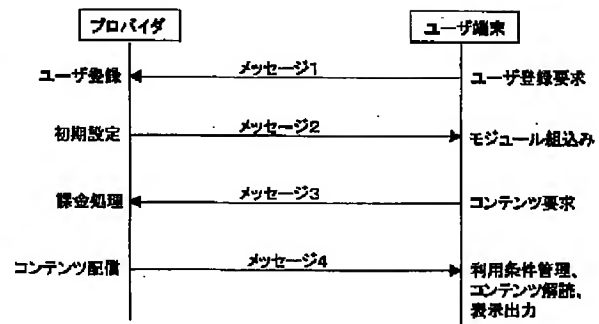
【図 4】



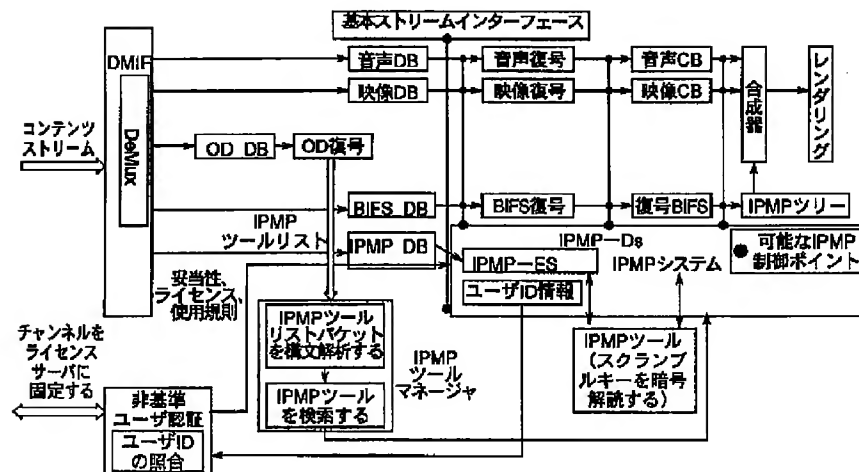
【図 5】



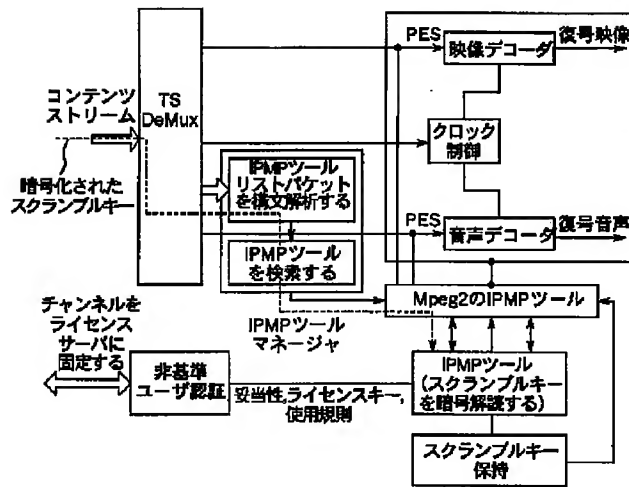
【図 10】



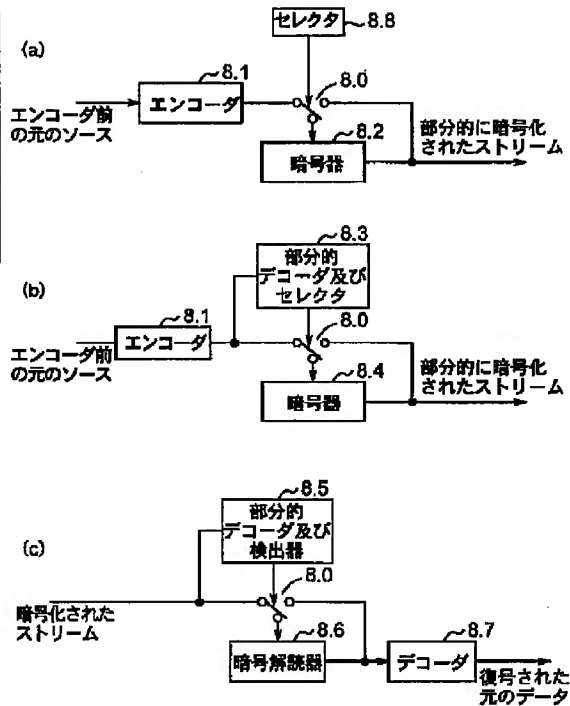
【図 6】



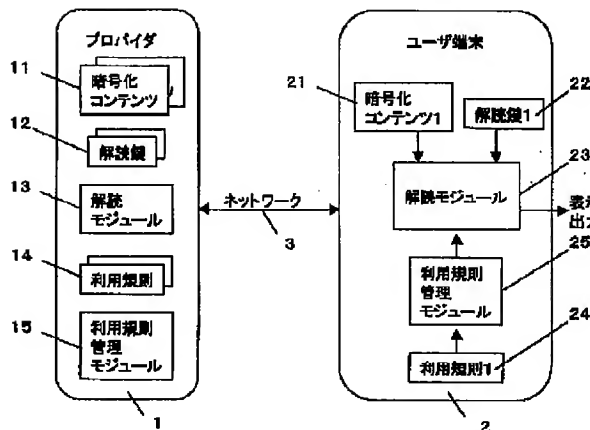
【図7】



【図8】



【図9】



【図11】

メッセージ1

メッセージID=	ユーザー登録
ユーザー名=	松下 太郎
支払い方法=	クレジットカード番号
ユーザー端末情報=	Windows OS

メッセージ2

メッセージID=	初期設定
ユーザーID=	XYZ
IPMP情報=	コンテンツリスト
IPMPツール情報=	解読モジュールID, ロケーション
IPMPツール情報=	利用規則管理モジュールID, ロケーション

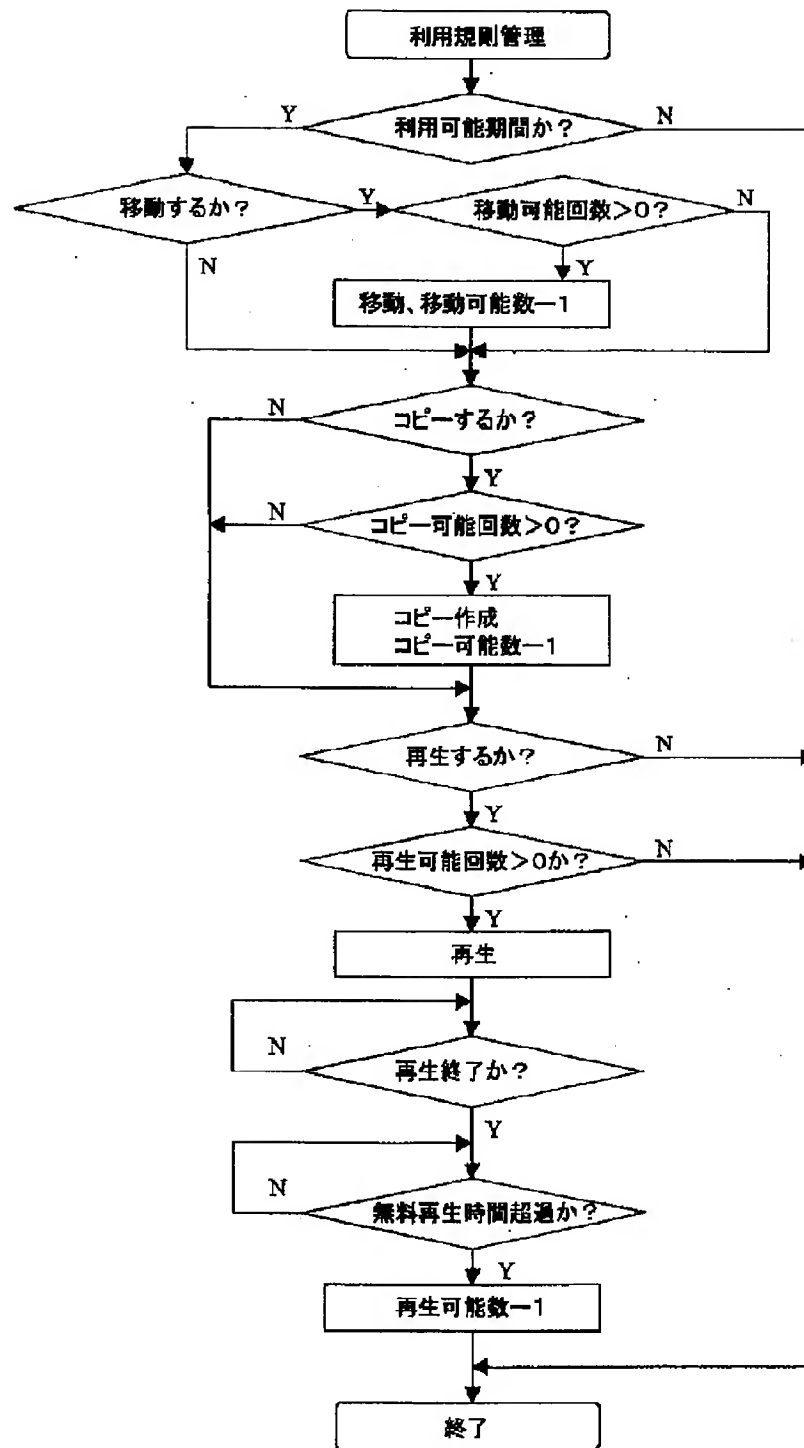
メッセージ3

メッセージID=	コンテンツ要求
ユーザーID=	XYZ
コンテンツ情報=	コンテンツ1ID

メッセージ4

メッセージID=	コンテンツ配信
IPMP情報=	利用規則1
IPMP情報=	解読鍵1
コンテンツ情報=	暗号化コンテンツ1

【図13】



フロントページの続き

(72)発明者 ジ・ミン

シンガポール534415シンガポール、タイ・
セン・アベニュー、ブロック1022、04-
3530番、タイ・セン・インダストリアル・
エステイト、パナソニック・シンガポール
研究所株式会社内

(72)発明者 妹尾 孝憲

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 小暮 拓世

大阪府寝屋川市田井西町4-12

Fターム(参考) 5J104 AA14 AA16 EA17 NA02 PA07

【公報種別】特許法第17条の2の規定による補正の掲載
 【部門区分】第7部門第3区分
 【発行日】平成17年10月13日(2005.10.13)

【公開番号】特開2003-78519(P2003-78519A)
 【公開日】平成15年3月14日(2003.3.14)
 【出願番号】特願2002-161440(P2002-161440)
 【国際特許分類第7版】

H 0 4 L 9/14

G 0 6 F 17/60

G 0 9 C 5/00

【F I】

H 0 4 L 9/00 6 4 1

G 0 6 F 17/60 1 4 2

G 0 6 F 17/60 3 0 2 E

G 0 6 F 17/60 5 1 2

G 0 9 C 5/00

【手続補正書】

【提出日】平成17年6月1日(2005.6.1)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置であって、

符号化技術を用いてコンテンツをコンテンツストリームに符号化する手段と、
 データ暗号化ツールを用いて当該符号化コンテンツストリームを暗号化する手段と、
 透かしツールを用いて当該コンテンツに透かし情報を埋め込む手段と、

上記ステップで用いられた当該コンテンツに関するコンテンツID及びIPMP(知的所有権管理保護)ツールリスト(IPMPツール情報)を作成する手段と、

各コンテンツストリームのヘッダとして保持すべきIPMPツールリストフラグを作成する手段と、

IPMPツールリストフラグ、次いでIPMPツールリスト、コンテンツID及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成する手段とを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項2】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置であって、

符号化技術を用いてコンテンツをコンテンツストリームに符号化する手段と、

データ暗号化ツール又は他のツールを用いた当該符号化コンテンツストリームを暗号化する手段と、

上記ステップで用いられた当該コンテンツに関するコンテンツID及びIPMP(知的所有権管理保護)ツールリスト(IPMPツール情報)を作成する手段と、

各コンテンツストリームのヘッダとして保持すべきIPMPツールリストフラグを作成する手段と、

IPMPツールリストフラグ、次いでIPMPツールリスト、コンテンツID及び実際の符号化

コンテンツストリームを含むコンテンツストリームを構成する手段とを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 3】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置であって、

符号化技術を用いてコンテンツをコンテンツストリームに符号化する手段と、

暗号化キーを有する暗号化ツール又は他のツールを用いて当該コンテンツストリームを暗号化する手段と、

より高いセキュリティのために別の暗号化キーを有する任意の暗号化ツールを用いて当該暗号化キーを暗号化する手段と、

当該コンテンツストリームと同一のストリームに保持されたIPMP情報に上記当該暗号化されたキーを埋め込む手段と、

上記ステップで使われた当該コンテンツに関するコンテンツID及びIPMP（知的所有権管理保護）ツールリスト（IPMPツール情報）を作成する手段と、

各コンテンツストリームのヘッダとして保持すべきIPMPツールリストフラグを作成する手段と、

IPMPツールリストフラグ、次いでIPMPツールリスト、コンテンツID及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成する手段とを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 4】

請求項 1 ないし 3 のいずれかにおいて、当該コンテンツに関するコンテンツID及びIPMPツールリストを作成するように、

IPMPツールIDを各コンテンツに割当てて、何れのツールをデータ保護に使用するかを表示する手段と、

位置タイプIDを各IPMPツールに割当てて、当該IPMPツールが入手可能である位置のタイプを通知する手段と、

フォーマットIDを割当てて、ダウンロードされたIPMPツールフォーマットを表示して、準拠IPMP端末がそれらのプラットフォームに基づいて選択及び検索することを可能にする手段と、

当該IPMPツールの位置を表示して、端末が当該IPMPツールを当該位置から取得することを可能にする手段を更に含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 5】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置であって、

IPMP端末のIPMPツールマネージャでコンテンツストリームの中を構文解析する手段と、

IPMPツールリストフラグ、コンテンツID及びIPMPツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該IPMPツールリストに基づいてIPMPツールを取得する手段とを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 6】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置であって、

IPMP端末のIPMPツールマネージャでコンテンツストリームの中を構文解析する手段と、

IPMPツールリストフラグ、コンテンツID及びIPMPツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該IPMPツールリストに基づいてIPMPツールを取得する手段と、

要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行う手段

と、

前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信する手段と、

前記ユーザ権利認証が成功した後、要求されたコンテンツの消費用の使用規則を取得する手段とを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 7】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置であって、

要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行う手段と、

前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信する手段と、

当該ライセンス又はキー情報をIPMP端末で構文解析する手段と、

当該ライセンス又はキー情報を当該IPMP端末のメモリに格納する手段と、

当該IPMP端末のIPMPツールマネージャでコンテンツストリームの中を構文解析する手段と、

IPMPツールリストフラグ、コンテンツID及びIPMPツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該IPMPツールリストに基づいてIPMPツールを取得する手段と、

IPMPツールリスト情報の当該部分と共に上記ステップで検索された当該IPMPツールを当該IPMP端末のメモリに格納する手段と、

当該メモリに格納された当該IPMPツールと共に当該ライセンス／キー情報を用いて当該コンテンツストリームを暗号解読及び復号する手段とを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 8】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置であって、

要求をコンテンツディストリビュータに送信して、ユーザ認証を行う手段と、

当該コンテンツディストリビュータからライセンス又はキー情報を受信する手段と、

当該ライセンス又はキー情報をIPMP端末で構文解析する手段と、

当該ライセンス又はキー情報を当該IPMP端末のメモリに格納する手段と、

当該IPMP端末のIPMPツールマネージャでコンテンツストリームの中を構文解析する手段と、

IPMPツールリストフラグ、コンテンツID及びIPMPツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該IPMPツールリストに基づいてIPMPツールを取得する手段と、

IPMPツールリスト情報の当該部分と共に上記ステップで検索された当該IPMPツールを当該IPMP端末のメモリに格納する手段と、

当該ライセンス又はキー情報を用いて当該IPMP情報内の当該暗号化されたキーを暗号解読する手段と、

コンテンツプロバイダ側で当該コンテンツを暗号化するために使用された暗号化キーを上記ステップから取得する手段と、

上記ステップから取得された当該暗号化キーを用いて当該コンテンツを暗号解読して、最初のコンテンツを取得する手段と、

当該最初のコンテンツを当該IPMP端末での再生のために復号する手段とを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 9】

請求項 5， 6， 7， 8 のいずれかにおいて、IPMPツールリストは、

IPMPツールの大部分に関するIPMPツールIDをテーブル状に定義しており、

当該テーブルに予約可能な未使用スペースがあり、
IPMPツールタイプとも呼ばれるIPMPツールのカテゴリとしてIPMPツールIDの一部が定義されており、
当該テーブルをIPMP端末に事前ロード、事前符号化又はダウンロードする手段と、
前記コンテンツストリーム内に保持された当該IPMPツールリストから当該IPMPツールIDを抽出する手段と、
前記コンテンツストリームに保持された当該IPMPツールリストに表示されたIPMPツール位置識別子を取得する手段と、
IPMPツール位置識別子に加えて、IPMPツールIDと共に、当該コンテンツストリームに保持されたIPMPツールフォーマットIDを取得する手段と、
適切なフォーマットであるIPMPツールを選択して、IPMP端末プラットフォームに適合させる手段と、
上記手段で取得された当該位置から当該IPMPツールを検索する手段とを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 10】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置であって、

予め定めたテーブルに基づいてIPMPツールリストを構築してコンテンツに使用されたIPMPツールの内容をIPMP端末に通知するように、

データ暗号解読、透かしなどのIPMPツールのカテゴリとして当該予め定めたテーブルからIPMPツールタイプIDを選択する手段と、

当該IPMPツールタイプIDの下である特定のアルゴリズムを有するある特定のIPMPツールに関して当該予め定めたテーブルからIPMPツールIDを選択する手段と、

当該予め定めたテーブルからIPMPツール位置IDを選択して、IPMPツールをダウンロード又は検索可能な場所を通知する手段と、

IPMPツールを遠隔で検索する場合、当該IPMPツールリストにURL位置を与える手段と

、
バイナリフォーマットにプリコンパイルされたIPMPツールの各セットに関するIPMPツールフォーマットIDを選択する手段とを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 11】

請求項 1, 2, 3 のいずれかにおいて、暗号化ツールを用いて事前符号化コンテンツストリームを暗号化するように、

イントラ符号化フレーム（I フレーム）などの事前符号化映像ストリームでキーアクセスユニットを探索する手段と、

すべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該キーアクセスユニットのみを暗号化して、暗号解読側の処理を高速化する手段とを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 12】

請求項 1, 2, 3 のいずれかにおいて、暗号化ツールを用いて事前符号化コンテンツストリームを暗号化するように、

事前符号化映像ストリーム又は音声ストリームで重要ビットを探索する手段と、

すべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該重要ビットのみを暗号化して、暗号解読側の処理を高速化する手段とを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 13】

請求項 11 において、選択されたアクセスユニット又は重要ビットに関して暗号化を部分的に行われた保護コンテンツストリームを復号する手段と、

予め定めた規則に基づいて暗号化されたビット又はアクセスユニットを探索して、所与のデータ暗号解読ツールを用いて前記ビット又はアクセスユニットを暗号解読する手段

とを含み、保護コンテンツを暗号解読して再生することを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 14】

請求項 1 ないし 3 のいずれかにおいて、指定インタフェースに従ってIPMPツールがされており、

当該インタフェースを含んだIPMP端末が構築され、

当該IPMPツールを検索して当該端末の当該インタフェースに適合させる手段を更に含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 15】

請求項 1 ないし 3 のいずれかにおいて、MPEG-4システムにある基本ストリームに対応付けられたデコーダ構成記述子に新しいストリームタイプを指定し、

MPEG-4のIPMP基本ストリームにIPMPツールを保持することを可能にしたことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 16】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法であって、

符号化技術を用いてコンテンツをコンテンツストリームに符号化するステップと、

データ暗号化ツールを用いて当該符号化コンテンツストリームを暗号化するステップと、

透かしツールを用いて当該コンテンツに透かし情報を埋め込むステップと、

上記ステップで用いられた当該コンテンツに関するコンテンツID及びIPMP（知的所有権管理保護）ツールリスト（IPMPツール情報）を作成するステップと、

各コンテンツストリームのヘッダとして保持すべきIPMPツールリストフラグを作成するステップと、

IPMPツールリストフラグ、次いでIPMPツールリスト、コンテンツID及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成するステップとを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項 17】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法であって、

符号化技術を用いてコンテンツをコンテンツストリームに符号化するステップと、

データ暗号化ツール又は他のツールを用いて当該符号化コンテンツストリームを暗号化するステップと、

上記ステップで用いた当該コンテンツに関するコンテンツID及びIPMP（知的所有権管理保護）ツールリスト（IPMPツール情報）を作成するステップと、

各コンテンツストリームのヘッダとして保持すべきIPMPツールリストフラグを作成するステップと、

IPMPツールリストフラグ、次いでIPMPツールリスト、コンテンツID及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成するステップとを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項 18】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法であって、

符号化技術を用いてコンテンツをコンテンツストリームに符号化するステップと、

暗号化キーを有する暗号化ツール又は他のツールを用いて当該コンテンツストリームを暗号化するステップと、

より高いセキュリティのために別の暗号化キーを有する任意の暗号化ツールを用いて当該暗号化キーを暗号化するステップと、

当該コンテンツストリームと同一のストリームに保持されたIPMP情報に上記当該暗号化されたキーを埋め込むステップと、

上記ステップで用いた当該コンテンツに関するコンテンツID及びIPMP（知的所有権管理保護）ツールリスト（IPMPツール情報）を作成するステップと、

各コンテンツストリームのヘッダとして保持すべきIPMPツールリストフラグを作成するステップと、

IPMPツールリストフラグ、次いでIPMPツールリスト、コンテンツID及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成するステップとを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項 19】

請求項 16, 17, 18 のいずれかにおいて、当該コンテンツに関するコンテンツID及びIPMPツールリストを作成するように、

IPMPツールIDを各コンテンツに割当てて、何れのツールをデータ保護に使用するかを表示するステップと、

位置タイプIDを各IPMPツールに割当てて、当該IPMPツールが入手可能である位置のタイプを通知するステップと、

フォーマットIDを割当てて、ダウンロードされたIPMPツールフォーマットを表示して、準拠IPMP端末がそれらのプラットフォームに基づいて選択及び検索することを可能にするステップと、

当該IPMPツールの位置を表示して、端末が当該IPMPツールを当該位置から取得することを可能にするステップとを更に含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項 20】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法であって、

IPMP端末のIPMPツールマネージャでコンテンツストリームの中を構文解析するステップと、

IPMPツールリストフラグ、コンテンツID及びIPMPツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該IPMPツールリストに基づいてIPMPツールを取得するステップとを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項 21】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法であって、

IPMP端末のIPMPツールマネージャでコンテンツストリームの中を構文解析するステップと、

IPMPツールリストフラグ、コンテンツID及びIPMPツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該IPMPツールリストに基づいてIPMPツールを取得するステップと、

要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行うステップと、

前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信するステップと、

前記ユーザ権利認証が成功した後、要求されたコンテンツの消費用の使用規則を取得するステップとを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項 22】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法であって、

要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行うステ

ップと、

前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信するステップと、

当該ライセンス又はキー情報をIPMP端末で構文解析するステップと、

当該ライセンス又はキー情報を当該IPMP端末のメモリに格納するステップと、

当該IPMP端末のIPMPツールマネージャでコンテンツストリームの中を構文解析するステップと、

IPMPツールリストフラグ、コンテンツID及びIPMPツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該IPMPツールリストに基づいてIPMPツールを取得するステップと、

IPMPツールリスト情報の当該部分と共に上記ステップで検索された当該IPMPツールを当該IPMP端末のメモリに格納するステップと、

当該メモリに格納された当該IPMPツールと共に当該ライセンス／キー情報を用いて当該コンテンツストリームを暗号解読及び復号するステップとを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項 2 3】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法であって、

要求をコンテンツディストリビュータに送宿して、ユーザ認証を行うステップと、

当該コンテンツディストリビュータからライセンス又はキー情報を受信するステップと、

当該ライセンス又はキー情報をIPMP端末で構文解析するステップと、

当該ライセンス又はキー情報を当該IPMP端末のメモリに格納するステップと、

当該IPMP端末のIPMPツールマネージャでコンテンツストリームの中を構文解析するステップと、

IPMPツールリストフラグ、コンテンツID及びIPMPツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該IPMPツールリストに基づいてIPMPツールを取得するステップと、

IPMPツールリスト情報の当該部分と共に上記ステップで検索された当該IPMPツールを当該IPMP端末のメモリに格納するステップと、

当該ライセンス又はキー情報を用いて当該IPMP情報内の当該暗号化されたキーを暗号解読するステップと、コンテンツプロバイダ側で当該コンテンツを上記ステップで暗号化するために使用された暗号化キーを取得するステップと、

上記ステップから取得された当該暗号化キーを用いて当該コンテンツを暗号解読して、最初のコンテンツを取得するステップと、

当該最初のコンテンツを当該IPMP端末で再生する為に復号するステップとを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項 2 4】

請求項 2 0， 2 1， 2 2， 2 3 のいずれかにおいて、ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該IPMPツールリストに基づいてIPMPツールを取得するように、

IPMPツールの大部分に関するIPMPツールIDをテーブルに定義されており、

今後の又は未知／専用のIPMPツールに使用されるべきIPMPツールIDに関する項目を当該テーブルに予約する余地があり、

IPMPツールタイプとも呼ばれるIPMPツールのカテゴリとしてIPMPツールIDの一部が定義されている、

当該テーブルをIPMP端末に事前ロード、事前符号化又はダウンロードするステップと、

前記コンテンツストリーム内に保持された当該IPMPツールリストから当該IPMPツールIDを抽出するステップと、

前記コンテンツストリームに保持された当該IPMPツールリストに表示されたIPMPツール位置識別子を取得するステップと、

IPMPツール位置識別子に加えて、IPMPツールIDと共に、当該コンテンツストリームに保持されたIPMPツールフォーマットIDを取得するステップと、

適切なフォーマットであるIPMPツールを選択して、IPMP端末プラットフォームに適合させるステップと、

上記手段で取得された当該位置から当該IPMPツールを検索するステップとを更に含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項 25】

請求項 20 ないし 23 のいずれかにおいて、予め定めたテーブルに基づいてIPMPツールリストを構築して、コンテンツに使用されたIPMPツールの内容をIPMP端末に通知するステップと、

対応するコンテンツストリームの前に当該IPMPツールリストを挿入するステップとを更に含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法

【請求項 26】

コンテンツプロバイダと利用者IPMP端末とを含むコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法であって、

予め定めたテーブルに基づいてIPMPツールリストを構築してコンテンツに使用されたIPMPツールの内容をIPMP端末に通知するように、

データ暗号解読、透かしなどのIPMPツールのカテゴリとして当該予め定めたテーブルからIPMPツールタイプIDを選択するステップと、

当該IPMPツールタイプIDの下である特定のアルゴリズムを有するある特定のIPMPツールに関して当該予め定めたテーブルからIPMPツールIDを選択するステップと、

当該予め定めたテーブルからIPMPツール位置IDを選択して、IPMPツールをダウンロード又は検索可能な場所を通知するステップと、

IPMPツールを遠隔で検索する場合、当該IPMPツールリストにURL位置を与えるステップと、

バイナリフォーマットにプリコンパイルされたIPMPツールの各セットに関するIPMPツールフォーマットIDを選択するステップとを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項 27】

請求項 16, 17, 18 のいずれかにおいて、暗号化ツールを用いて事前符号化コンテンツストリームを暗号化するように、

イントラ符号化フレーム（Iフレーム）などの事前符号化映像ストリームでキーアクセスユニットを探索するステップと、

すべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該キーアクセスユニットのみを暗号化して、暗号解読側の処理を高速化するステップとを更に含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項 28】

請求項 16, 17, 18 のいずれかにおいて、暗号化ツールを用いて事前符号化コンテンツストリームを暗号化するように、

事前符号化映像ストリーム又は音声ストリームで重要ビットを探索するステップと、

すべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該重要ビットのみを暗号化して、暗号解読側の処理を高速化するステップとを更に含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項 29】

請求項 27 において、選択されたアクセスユニット又は重要ビットに関して暗号化を部

分的に行うように、

保護コンテンツストリームを復号するステップと、
予め定めた規則に基づいて暗号化されたビット又はアクセスユニットを探索して、所与のデータ暗号解読ツールを用いて前記ビット又はアクセスユニットを暗号解読するステップとを含み、保護コンテンツを暗号解読して再生することを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項30】

請求項16ないし18のいずれかにおいて、MPEG-4システムにある基本ストリームに対応付けられたデコーダ構成記述子に新しいストリームタイプを指定して、

MPEG-4のIPMP基本ストリームにIPMPツールを保持することを可能にしたことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの方法。

【請求項31】

請求項1ないし3のいずれかにおいて、暗号化されたコンテンツと、その解読鍵と、解読モジュールと、コンテンツの利用規則と、利用規則管理モジュールを持つコンテンツプロバイダは、ネットワークを通じて接続されたユーザIPMP端末に送るメッセージ中に、解読モジュールの識別子とその存在する場所を示す情報及び利用規則管理モジュールの識別子とその存在する場所を示す情報を含めることにより、ユーザIPMP端末はコンテンツプロバイダから受信したメッセージに基づいて著作権保護システムの更新を行い、更新した解読モジュールと更新した利用規則管理モジュールを含むことにより、前記コンテンツプロバイダが意図する利用規則に従ってコンテンツの解読視聴を行うことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項32】

請求項1ないし3のいずれかにおいて、暗号化されたコンテンツと、その解読鍵と、解読モジュールと、コンテンツの利用規則と、利用規則管理モジュールを持つコンテンツプロバイダとネットワークを通じて接続されたユーザIPMP端末は、前記コンテンツプロバイダから利用規則管理モジュールを受け取って自身に組み込み、これを用いて、前記コンテンツプロバイダから受け取る著作権保護情報の中にある、コンテンツの利用規則に従い、前記コンテンツプロバイダから受け取るコンテンツの再生を行うことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項33】

請求項31において、利用規則は、コンテンツの利用可能期間、無料再生可能時間、再生可能回数、コピー可能回数、移動可能回数のいずれかを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項34】

請求項31において、前記コンテンツプロバイダからユーザIPMP端末に送られるメッセージは、メッセージ項目名と直後に続くメッセージ項目の倍の組で構成され、ユーザIPMP端末に送るメッセージ項目の順序を問わないことを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項35】

請求項31または32において、ユーザIPMP端末からコンテンツプロバイダに送られるメッセージは、ユーザIPMP端末情報を含むことにより、ユーザIPMP端末に適合するモジュールをコンテンツプロバイダから受信することが出来ることを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項36】

請求項12において、選択されたアクセスユニット又は重要ビットに関して暗号化を部分的に行われた保護コンテンツストリームを復号する手段と、予め定めた規則に基づいて暗号化されたビット又はアクセスユニットを探索して、所与のデータ暗号解読ツールを用いて前記ビット又はアクセスユニットを暗号解読する手段とを含み、保護コンテンツを暗号解読して再生することを特徴とするコンテンツ提供及び保護用の柔軟及び共通IPMPシステムの装置。

【請求項 37】

請求項 28 において、選択されたアクセスユニット又は重要ビットに関して暗号化を部分的に行うように、

保護コンテンツストリームを復号するステップと、

予め定めた規則に基づいて暗号化されたビット又はアクセスユニットを探索して、所与のデータ暗号解読ツールを用いて前記ビット又はアクセスユニットを暗号解読するステップとを含み、保護コンテンツを暗号解読して再生することを特徴とするコンテンツ提供及び保護用の柔軟及び共通 IPMP システムの方法。

【請求項 38】

請求項 32 において、利用規則は、コンテンツの利用可能期間、無料再生可能時間、再生可能回数、コピー可能回数、移動可能回数のいずれかを含むことを特徴とするコンテンツ提供及び保護用の柔軟及び共通 IPMP システムの装置。

【請求項 39】

請求項 32 において、前記コンテンツプロバイダからユーザ IPMP 端末に送られるメッセージは、メッセージ項目名と直後に続くメッセージ項目の倍の組で構成され、ユーザ IPMP 端末に送るメッセージ項目の順序を問わないことを特徴とするコンテンツ提供及び保護用の柔軟及び共通 IPMP システムの装置。

【請求項 40】

請求項 32 において、ユーザ IPMP 端末からコンテンツプロバイダに送られるメッセージは、ユーザ IPMP 端末情報を含むことにより、ユーザ IPMP 端末に適合するモジュールをコンテンツプロバイダから受信することが出来ることを特徴とするコンテンツ提供及び保護用の柔軟及び共通 IPMP システムの装置。